И. М. ВИНОГРАДОВ

ОСНОВЫ ТЕОРИИ ЧИСЕЛ

КНИГА ДОЛЖНА БЫТЬ
ВОЗВРАЩЕНА НЕ ПОЗЖЕ
УКАЗАННОГО ЗДЕСЬ СРОКА

Колич. предыд. выдач _____

6472

Зак. 23-Д

806

Академик И. М. ВИНОГРАДОВ

511
В 49

ОСНОВЫ ТЕОРИИ ЧИСЕЛ

ИЗДАНИЕ ШЕСТОЕ,
ИСПРАВЛЕННОЕ

Допущено Министерством высшего образования СССР в качестве учебника для физико-математических факультетов государственных университетов

МОСКОВСКИЙ
Физико-Технический
Институт
БИБЛИОТЕКА

129350 экз.

ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ТЕХНИКО-ТЕОРЕТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1952 ЛЕНИНГРАД

ПРОВЕРЕНО
1988 г.

11-5-2

Редактор *А. З. Рыжик.*

Техн. редактор *М. Д. Суховцева.* Корректор *И. С. Варшавская.*

Подписано к печати 26/XII 1951 г. Бумага 84×108/32. 2,813 бум. л. 9,23 печ. л. 10,83 уч.-изд. л. 42,591 тип. зн. в печ. л. Т-09549. Тираж 10 000 экз. Цена книги 3 р. 80 к. Переплёт 2 р. Заказ № 1362

16-я типография Главполиграфиздата при Совете Министров СССР. Москва, Трёхпрудный пер., 9.

ОГЛАВЛЕНИЕ.

Замеченные опечатки
(допущены не вне типографии)

Страница	Строка	Напечатано	Следует читать
23	11 св.	когда	тогда
93	13 св.	$(xy)^{ab} - 1 \pmod m$	$(xy)^{ab} \equiv 1 \pmod m$
100	1 св.	$g\frac{c}{q} \equiv 1 \pmod m$	$g^{\frac{c}{q}} \equiv 1 \pmod m$
116	15 св.	$(3 \ln N) < N$	$(3 \ln N)^k < N$
123	1 св.	$\sum_{d^1 \backslash a_1}$	$\sum_{d_1 \backslash a_1}$
124	5 св.	$\frac{a_2 \quad 1}{}$	$\frac{a_2 + 1}{}$
152	5 св.	2	2^k

Зак. 1362

ГЛАВА ПЯТАЯ.

СРАВНЕНИЯ ВТОРОЙ СТЕПЕНИ.

§ 1. Общие теоремы (71). § 2. Символ Лежандра (73). § 3. Символ Якоби (78). § 4. Случай составного модуля (82). Вопросы к главе V (84). Численные примеры к главе V (90).

ГЛАВА ШЕСТАЯ.

ПЕРВООБРАЗНЫЕ КОРНИ И ИНДЕКСЫ.

§ 1. Общие теоремы (92). § 2. Первообразные корни по модулям p^α и $2p^\alpha$ (93). § 3. Разыскание первообразных корней по модулям p^α и $2p^\alpha$ (95). § 4. Индексы по модулям p^α и $2p^\alpha$ (96). § 5. Следствия предыдущей теории (99). § 6. Индексы по модулю 2^α (102). § 7. Индексы по любому составному модулю (104). Вопросы к главе VI (106). Численные примеры к главе VI (112).

Решения вопросов.

Решения к главе I (114). Решения к главе II (118).
Решения к главе III (132). Решения к главе IV (143).
Решения к главе V (149). Решения к главе VI (159).

Ответы к численным примерам.

Ответы к главе I (170). Ответы к главе II (170).
Ответы к главе III (170). Ответы к главе IV (170).
Ответы к главе V (171). Ответы к главе VI (171).

Таблицы индексов 173

Таблица простых чисел < 4000 и их наименьших первообразных корней 179

ПРЕДИСЛОВИЕ К ПЯТОМУ ИЗДАНИЮ.

Ряд русских математиков — Чебышев, Коркин, Золотарёв, Марков, Вороной и другие — занимался теорией чисел. Ознакомиться с содержанием классических работ этих замечательных учёных можно по книжке Б. Н. Делоне «Петербургская школа теории чисел».

Советские математики, работающие в области теории чисел, продолжая славные традиции своих предшественников, создали новые мощные методы, позволившие получить ряд первоклассных результатов; в разделе теории чисел книги «Математика в СССР за 30 лет» можно найти сведения о достижениях советских учёных в области теории чисел, а также соответствующие библиографические данные.

В моей книге даётся систематическое изложение основ теории чисел в объёме университетского курса. Значительное количество задач вводит читателя в круг некоторых новых идей в области теории чисел.

Настоящее пятое издание книги значительно отличается от четвёртого. Ряд изменений, способствующих большей простоте изложения, внесён во все главы книги. Особо значительными изменениями являются объединение прежних глав IV и V в одну главу IV (благодаря чему число глав сократилось до шести), а также новое, более простое доказательство существования первообразных корней.

Существенно переработаны вопросы, помещённые в конце каждой главы. Порядок следования вопросов теперь приведён в полное соответствие с порядком расположения теоретического материала. Введены некоторые новые вопросы; однако число номеров вопросов

значительно сокращено. Последнее достигнуто путём объединения под названиями a, b, c, ... ранее самостоятельных вопросов, близких по методу решения или по содержанию. Пересмотрены все решения вопросов; в ряде случаев эти решения упрощены или заменены лучшими. Особенно сильные изменения внесены в решения вопросов, касающихся распределения вычетов и невычетов n-й степени и первообразных корней, а также оценок соответствующих тригонометрических сумм.

И. М. Виноградов

ГЛАВА ПЕРВАЯ.

ТЕОРИЯ ДЕЛИМОСТИ.

§ 1. Основные понятия и теоремы.

a. Теория чисел занимается изучением свойств целых чисел. Целыми мы будем называть не только числа натурального ряда 1, 2, 3, ... (положительные целые), но также нуль и отрицательные целые -1, -2, -3, ...

Как правило, при изложении теоретического материала мы будем обозначать буквами только целые числа. Случаи, когда буквы могут обозначать и не целые числа, если последнее не будет ясно само по себе, мы будем особо оговаривать.

Сумма, разность и произведение двух целых a и b будут также целыми, но частное от деления a на b (если b не равно нулю) может быть как целым, так и не целым.

b. В случае, когда частное от деления a на b — целое, обозначая его буквою q, имеем $a = bq$, т. е. *a равно произведению b на целое*. Мы говорим тогда, что *a делится* на b или что *b делит a*. При этом a называем *кратным* числа b и b — *делителем* числа a. То обстоятельство, что b делит a, записывается так: $b \backslash a$.

Имеют место две следующие теоремы.

1. *Если a кратно m, m кратно b, то a кратно b.*

Действительно, из $a = a_1 m$, $m = m_1 b$ следует $a = a_1 m_1 b$, где $a_1 m_1$ — целое. А это и доказывает теорему.

2. *Если в равенстве вида $k + l + \ldots + n = p + q + \ldots + s$ относительно всех членов, кроме какого-либо одного,*

известно, что они кратны b, то и этот один член кратен b.

Действительно, пусть таким членом будет k. Имеем

$$l = l_1 b, \ \ldots, \ n = n_1 b, \ p = p_1 b, \ q = q_1 b, \ \ldots, \ s = s_1 b,$$
$$k = p + q + \ldots + s - l - \ldots - n =$$
$$= (p_1 + q_1 + \ldots + s_1 - l_1 - \ldots - n_1) b.$$

А это и доказывает теорему.

c. В общем случае, включающем, как частный, и случай, когда a делится на b, имеем теорему:

Всякое целое a представляется единственным способом через положительное целое b в форме

$$a = bq + r; \quad 0 \leqslant r < b.$$

Действительно, одно представление a в такой форме получим, взяв bq равным наибольшему кратному числа b, не превосходящему a. Допустив, что также $a = bq_1 + r_1$, $0 \leqslant r_1 < b$, получим $0 = b(q - q_1) + r - r_1$, откуда следует (2, b), что $r - r_1$ кратно b. Но ввиду $|r - r_1| < b$ последнее возможно лишь при $r - r_1 = 0$, т. е. при $r = r_1$, откуда вытекает также $q = q_1$.

Число q называется *неполным частным*, а число r — *остатком* от деления a на b.

Пример. Пусть $b = 14$. Имеем

$$177 = 14 \cdot 12 + 9; \qquad 0 < 9 < 14,$$
$$-64 = 14 \cdot (-5) + 6; \qquad 0 < 6 < 14,$$
$$154 = 14 \cdot 11 + 0; \qquad 0 = 0 < 14.$$

§ 2. Общий наибольший делитель.

a. В дальнейшем мы будем рассматривать лишь положительные делители чисел. Всякое целое, делящее одновременно целые $a, b, \ldots, l$, называется их *общим делителем*. Наибольший из общих делителей называется *общим наибольшим делителем* и обозначается символом $(a, b, \ldots, l)$. Ввиду конечности числа общих делителей существование общего наибольшего делителя очевидно. Если $(a, b, \ldots, l) = 1$, то $a, b, \ldots, l$ называются *взаимно простыми*. Если каждое из чисел $a, b, \ldots, l$ взаимно просто с каждым другим из них, то $a, b, \ldots, l$ называются *попарно простыми*. Очевидно, числа попарно простые всегда и взаимно простые; в случае же двух чисел понятия «попарно простые» и «взаимно простые» совпадают.

Примеры. Числа 6, 10, 15 ввиду $(6, 10, 15) = 1$ — взаимно простые. Числа 8, 13, 21 ввиду $(8, 13) = (8, 21) = (13, 21) = 1$ — попарно простые.

b. Сначала займёмся общими делителями двух чисел.

1. *Если a кратно b, то совокупность общих делителей чисел a и b совпадает с совокупностью делителей одного b; в частности, $(a, b) = b$.*

Действительно, всякий общий делитель чисел a и b является делителем и одного b. Обратно, раз a кратно b, то (1, b, § 1) всякий делитель числа b является также делителем числа a, т. е. он будет общим делителем чисел b и a. Таким образом совокупность общих делителей чисел a и b совпадает с совокупностью делителей одного b. А так как наибольший делитель числа b есть само b, то $(a, b) = b$.

2. *Если*

$$a = bq + c,$$

то совокупность общих делителей чисел a и b совпадает с совокупностью общих делителей чисел b и c; в частности, $(a, b) = (b, c)$.

Действительно, написанное выше равенство показывает, что всякий общий делитель чисел a и b делит также и c (2, b, § 1) и, следовательно, является общим делителем чисел b и c. Обратно, то же равенство показывает, что всякий общий делитель чисел b и c делит a и, следовательно, является общим делителем чисел a и b. Таким образом общие делители чисел a и b суть те же, что и общие делители чисел b и c; в частности, должны совпадать и наибольшие из этих делителей, т. е. $(a, b) = (b, c)$.

c. Для разыскания общего наибольшего делителя, а также для вывода его важнейших свойств применяется *алгоритм Эвклида*. Последний состоит в нижеследующем.

Пусть a и b — положительные целые. Согласно c, § 1 находим ряд равенств:

$$\left.\begin{aligned} a &= bq_1 + r_2, & 0 < r_2 < b,\\ b &= r_2q_2 + r_3, & 0 < r_3 < r_2,\\ r_2 &= r_3q_3 + r_4, & 0 < r_4 < r_3,\\ &\dots\dots\dots\dots\dots\dots\dots\\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, & 0 < r_n < r_{n-1},\\ r_{n-1} &= r_nq_n, \end{aligned}\right\} \qquad (1)$$

заканчивающийся, когда получаем некоторое $r_{n+1} = 0$. Последнее неизбежно, так как ряд b, r_2, r_3, ... как ряд убывающих целых не может содержать более чем b положительных.

d. Рассматривая равенства (1), идя сверху вниз, убеждаемся (b), что общие делители чисел a и b одинаковы с общими делителями чисел b и r_2, далее одинаковы с общими делителями чисел r_2 и r_3, чисел r_3 и r_4, ..., чисел r_{n-1} и r_n, наконец, с делителями одного числа r_n. Одновременно с этим имеем

$$(a,\ b) = (b,\ r_2) = (r_2,\ r_3) = \dots = (r_{n-1},\ r_n) = r_n.$$

Мы приходим к следующим результатам.

1. *Совокупность общих делителей чисел a и b совпадает с совокупностью делителей их общего наибольшего делителя.*

2. *Этот общий наибольший делитель равен r_n, т. е. последнему не равному Нулю остатку алгоритма Эвклида.*

Пример. Применим алгоритм Эвклида к отысканию (525, 231). Находим (вспомогательные вычисления приведены слева)

525 | 231		$525 = 231 \cdot 2 + 63,$
462 | 2		
231 | 63		$231 = 63 \cdot 3 + 42,$
189 | 3		
63 | 42		$63 = 42 \cdot 1 + 21,$
42 | 1		
42 | 21		$42 = 21 \cdot 2.$
42 | 2		
0		

Здесь последний положительный остаток есть $r_4 = 21$. Значит, $(525,\ 231) = 21$.

e. 1. *Обозначая буквою m любое положительное целое, имеем $(am,\ bm) = (a,\ b)m$.*

2. *Обозначая буквою δ любой общий делитель чисел a и b, имеем $\left(\frac{a}{\delta},\ \frac{b}{\delta}\right) = \frac{(a,\ b)}{\delta}$; в частности, имеем $\left(\frac{a}{(a,\ b)},\ \frac{b}{(a,\ b)}\right) = 1$, т. е. частные от деления двух чисел на их общий наибольший делитель суть числа взаимно простые.*

Действительно, умножим равенства (1) почленно на m. Получим новые равенства, где вместо a, b, r_2, ..., r_n будут стоять am, bm, r_2m, ..., r_nm. Поэтому $(am,\ bm) = r_nm$, и таким образом верно утверждение 1.

Применяя утверждение 1, находим

$$(a,\ b) = \left(\frac{a}{\delta}\delta,\ \frac{b}{\delta}\delta\right) = \left(\frac{a}{\delta},\ \frac{b}{\delta}\right)\delta;$$

отсюда следует утверждение 2.

f. 1. *Если $(a,\ b) = 1$, то $(ac,\ b) = (c,\ b)$.*

Действительно, $(ac,\ b)$ делит ac и bc, значит (1, d), оно делит и $(ac,\ bc)$, ввиду 1, e равное c; но $(ac,\ b)$ делит и b, поэтому оно делит и $(c,\ b)$. Обратно, $(c,\ b)$ делит ac и b, поэтому оно делит и $(ac,\ b)$. Таким образом $(ac,\ b)$ и $(c,\ b)$ взаимно делят друг друга и, следовательно, равны между собою.

2. *Если $(a,\ b) = 1$ и ac делится на b, то c делится на b.*

Действительно, ввиду $(a,\ b) = 1$ имеем $(ac,\ b) = (c,\ b)$. Но раз ac кратно b, то (1, b) имеем $(ac,\ b) = b$, значит, и $(c,\ b) = b$, т. е. c кратно b.

3. *Если каждое a_1, a_2, ..., a_m взаимно просто с каждым b_1, b_2, ..., b_n, то и произведение $a_1a_2 \dots a_m$ взаимно просто с произведением $b_1b_2 \dots b_n$.*

Действительно (теорема 1), имеем

$$(a_1a_2a_3 \dots a_m,\ b_k) = (a_2a_3 \dots a_m,\ b_k) =$$
$$= (a_3 \dots a_m,\ b_k) = \dots = (a_m,\ b_k) = 1,$$

и далее, полагая для краткости $a_1a_2 \dots a_m = A$, точно таким же путём найдём

$$(b_1b_2b_3 \dots b_n, A) = (b_2b_3 \dots b_n, A) = \\ = (b_3 \dots b_n, A) = \dots = (b_n, A) = 1.$$

g. Задача отыскания общего наибольшего делителя более чем двух чисел сводится к таковой для двух чисел. Именно, чтобы найти общий наибольший делитель чисел $a_1, a_2, \dots, a_n$, составляем ряд чисел:

$$(a_1, a_2) = d_2, \ (d_2, a_3) = d_3, \ (d_3, a_4) = d_4, \ \dots, \ (d_{n-1}, a_n) = d_n.$$

Число d_n и будет общим наибольшим делителем всех данных чисел.

Действительно (1, d), общие делители чисел a_1 и a_2 совпадают с делителями d_2; поэтому общие делители чисел a_1, a_2 и a_3 совпадают с общими делителями чисел d_2 и a_3, т. е. совпадают с делителями d_3. Далее убедимся, что общие делители чисел a_1, a_2, a_3, a_4 совпадают с делителями d_4 и т. д. и, наконец, что общие делители чисел a_1, a_2, $\dots$, a_n совпадают с делителями d_n. А так как наибольший делитель d_n есть само d_n, то оно будет общим наибольшим делителем чисел a_1, a_2, $\dots$, a_n.

Просматривая приведённое доказательство, убеждаемся, что теорема 1, d верна и для более чем двух чисел. Верны также и теоремы 1, e и 2, e, потому что от умножения на m или разделения на b всех чисел $a_1, a_2, \dots, a_n$ точно так же и все $d_2, d_3, \dots, d_n$ умножатся на m или разделятся на b.

§ 3. Общее наименьшее кратное.

a. Всякое целое, кратное всех данных чисел, называется их *общим кратным*. Наименьшее положительное общее кратное называется *общим наименьшим кратным*.

b. Сначала займёмся общим наименьшим кратным двух чисел. Пусть M — какое-либо общее кратное целых

a и b. Так как оно кратно a, то $M = ak$, где k — целое. Но M кратно и b, поэтому целым должно быть и

$$\frac{ak}{b},$$

что, полагая $(a, b) = d$, $a = a_1d$, $b = b_1d$, можно представить в виде $\frac{a_1k}{b_1}$, где $(a_1, b_1) = 1$ (2, e, § 2). Поэтому (2, f, § 2) k должно делиться на b_1, $k = b_1t = \frac{b}{d}t$, где t — целое. Отсюда

$$M = \frac{ab}{d}t.$$

Обратно, очевидно, что всякое M такой формы кратно как a, так и b, и, таким образом, эта форма даёт общий вид всех общих кратных чисел a и b.

Наименьшее положительное из этих кратных, т. е. общее наименьшее кратное, получим при $t = 1$. Оно будет

$$m = \frac{ab}{d}.$$

Введя m, можно полученную для M формулу переписать так:

$$M = mt.$$

Последнее и предпоследнее равенства приводят к теоремам:

1. *Общие кратные двух чисел совпадают с кратными их общего наименьшего кратного.*

2. *Общее наименьшее кратное двух чисел равно их произведению, делённому на их общий наибольший делитель.*

c. Пусть требуется найти общее наименьшее кратное более чем двух чисел $a_1, a_2, \dots, a_n$. Обозначая вообще символом $[a, b]$ общее наименьшее кратное чисел a и b, составим ряд чисел:

$$[a_1, a_2] = m_2, \ [m_2, a_3] = m_3, \ \dots, \ [m_{n-1}, a_n] = m_n.$$

Полученное таким путём m_n и будет общим наименьшим кратным всех данных чисел.

d. Весьма простой закон образования подходящих дробей легко найдём, замечая, что δ_s $(s>1)$ получается из δ_{s-1} заменой в буквенном выражении для δ_{s-1} числа q_{s-1} на $q_{s-1}+\frac{1}{q_s}$.

Действительно, полагая для единообразия $P_0=1$, $Q_0=0$, мы можем подходящие дроби последовательно представить в следующем виде (здесь равенство $\frac{A}{B}=\frac{P_s}{Q_s}$ пишем, желая обозначить A символом P_s, а B символом Q_s):

$$\delta_1=\frac{q_1}{1}=\frac{P_1}{Q_1},\quad \delta_2=\frac{q_1+\frac{1}{q_2}}{1}=\frac{q_2q_1+1}{q_2\cdot 1+0}=\frac{q_2P_1+P_0}{q_2Q_1+Q_0}=\frac{P_2}{Q_2},$$

$$\delta_3=\frac{\left(q_2+\frac{1}{q_3}\right)P_1+P_0}{\left(q_2+\frac{1}{q_3}\right)Q_1+Q_0}=\frac{q_3P_2+P_1}{q_3Q_2+Q_1}=\frac{P_3}{Q_3}$$

и т. д. и вообще

$$\delta_s=\frac{q_sP_{s-1}+P_{s-2}}{q_sQ_{s-1}+Q_{s-2}}=\frac{P_s}{Q_s}.$$

Таким образом числители и знаменатели подходящих дробей мы можем последовательно вычислять по формулам

$$\left.\begin{aligned}P_s&=q_sP_{s-1}+P_{s-2},\\ Q_s&=q_sQ_{s-1}+Q_{s-2}.\end{aligned}\right\}\qquad(2)$$

Эти вычисления полезно производить по следующей схеме:

q_s		q_1	q_2	$\cdots$			q_s	$\cdots$		q_n
P_s	1	q_1	P_2	$\cdots$	P_{s-2}	P_{s-1}	P_s	$\cdots$	P_{n-1}	a
Q_s	0	1	Q_2	$\cdots$	Q_{s-2}	Q_{s-1}	Q_s	$\cdots$	Q_{n-1}	b

Пример. Разложим в непрерывную дробь число $\frac{105}{38}$. Здесь

$$\begin{array}{r|l}105&38\\76&2\\\hline 29&1\\29&9\\27&3\\\hline 2&4\\8&\\\hline 2&1\\2&2\\\hline 0&\end{array}\qquad \frac{105}{38}=2+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{4+\frac{1}{2}}}}.$$

Поэтому указанная выше схема даёт:

q_s		2	1	3	4	2
P_s	1	2	3	11	47	105
Q_s	0	1	1	4	17	38

129350

e. Рассмотрим разность $\delta_s-\delta_{s-1}$ соседних подходящих дробей. При $s>1$ находим

$$\delta_s-\delta_{s-1}=\frac{P_s}{Q_s}-\frac{P_{s-1}}{Q_{s-1}}=\frac{h_s}{Q_sQ_{s-1}},$$

где $h_s=P_sQ_{s-1}-Q_sP_{s-1}$; подставляя же вместо P_s и Q_s их выражения (2) и делая очевидные упрощения, получим $h_s=-h_{s-1}$. Последнее в соединении с $h_1=q_1\cdot 0-1\cdot 1=-1$ даёт $h_s=(-1)^s$. Итак,

$$P_sQ_{s-1}-Q_sP_{s-1}=(-1)^s\qquad(s>0),\qquad(3)$$

$$\delta_s-\delta_{s-1}=\frac{(-1)^s}{Q_sQ_{s-1}}\qquad(s>1).\qquad(4)$$

МОСКОВСКИЙ Физико-Технический Институт БИБЛИОТЕКА

Пример. В таблице примера, приведённого в d, имеем

$$105 \cdot 17 - 38 \cdot 47 = (-1)^5 = -1.$$

f. Из (3) следует, что (P_s, Q_s) делит $(-1)^s = \pm 1$ (2, b, § 1). Поэтому $(P_s, Q_s) = 1$, т. е. *подходящие дроби* $\frac{P_s}{Q_s}$ *несократимы.*

g. При δ_s, не равном α (т. е. исключается случай, когда, при рациональном α, δ_s является последней подходящей дробью), исследуем знак разности $\delta_s - \alpha$. Очевидно, δ_s получается заменой a_s на q_s в выражении (1) для α. Но, как видно из a, от такой замены

a_s уменьшится,
a_{s-1} увеличится,
a_{s-2} уменьшится,
. . . . . .
α при нечётном s уменьшится, при чётном s увеличится.

Поэтому $\delta_s - \alpha < 0$ при нечётном s и $\delta_s - \alpha > 0$ при чётном s, и следовательно, знак $\delta_s - \alpha$ совпадает со знаком $(-1)^s$.

h. *Имеем*

$$|\alpha - \delta_{s-1}| < \frac{1}{Q_s Q_{s-1}}.$$

Действительно, при $\delta_s = \alpha$ это утверждение следует (со знаком равенства) из (4). При δ_s, не равном α, оно следует (со знаком неравенства) из (4) и из того обстоятельства, что, ввиду g, $\delta_s - \alpha$ и $\delta_{s-1} - \alpha$ имеют разные знаки.

§ 5. Простые числа.

a. Число 1 имеет только один положительный делитель, именно 1. В этом отношении число 1 в ряде натуральных чисел стоит особо.

Всякое целое, большее 1, имеет не менее двух делителей, именно 1 и самого себя; если этими делителями исчерпываются все положительные делители целого числа, то оно называется *простым*. Целое > 1, имеющее кроме 1 и самого себя другие положительные делители, называется *составным*.

b. *Наименьший отличный от единицы делитель целого, большего единицы, есть число простое.*

Действительно, пусть q — наименьший отличный от единицы делитель целого $a > 1$. Если бы q было составным, то оно имело бы некоторый делитель q_1 с условием $1 < q_1 < q$; но число a, делясь на q, должно было бы делиться и на q_1 (1, b, § 1), а это противоречит нашему предположению относительно числа q.

c. *Наименьший отличный от единицы делитель составного числа a (согласно b он будет простым) не превосходит* $\sqrt{a}$.

Действительно, пусть q — этот делитель, тогда $a = qa_1$, $a_1 > q$, откуда, перемножая и сокращая на a_1, получим $a > q^2$, $q < \sqrt{a}$.

d. *Число простых чисел бесконечно велико.*

Справедливость этой теоремы следует из того, что, какова бы ни была различные простые $p_1, p_2, \ldots, p_k$, можно получить новое простое, среди них не заключающееся. Таковым будет простой делитель суммы $p_1 p_2 \ldots p_k + 1$, который, деля всю сумму, не может совпадать ни с одним из простых $p_1, p_2, \ldots, p_k$ (2, b, § 1).

e. Для составления таблицы простых чисел, не превосходящих данного N, существует простой способ, называемый *решетом Эратосфена*. Он состоит в нижеследующем.

Выписываем числа

$$1, 2, \ldots, N. \qquad (1)$$

Первое большее единицы число этого ряда есть 2; оно делится только на 1 и на самого себя, следовательно, оно простое.

Вычеркнем из ряда (1) (как составные) все числа, кратные 2, кроме самого 2. Первое следующее за 2 невычеркнутое число будет 3; оно не делится на 2 (иначе оно оказалось бы вычеркнутым), следовательно,

3 делится только на 1 и на самого себя, а потому оно также будет простым.

Вычёркиваем из ряда (1) все числа, кратные 3, кроме самого 3. Первое следующее за 3 невычеркнутое число будет 5; оно не делится ни на 2, ни на 3 (иначе оно оказалось бы вычеркнутым). Следовательно, 5 делится только на 1 и на самого себя, а потому оно также будет простым.

И т. д.

Когда указанным способом уже вычеркнуты все числа, кратные простых, меньших простого p, то все невычеркнутые, меньшие p^2, будут простые. Действительно, всякое составное a, меньшее p^2, нами уже вычеркнуто, как кратное его наименьшего простого делителя, который $\leqslant \sqrt{a} < p$. Отсюда следует:

1. *Приступая к вычёркиванию кратных простого p, это вычёркивание следует начинать с p^2.*

2. *Составление таблицы простых чисел $\leqslant N$ закончено, как только вычеркнуты все составные кратные простых, не превосходящих $\sqrt{N}$.*

§ 6. Единственность разложения на простые сомножители.

a. *Всякое целое a или взаимно просто с данным простым p, или же делится на p.*

Действительно, (a, p), будучи делителем p, может быть равно или 1, или p. В первом случае a взаимно просто с p, во втором a делится на p.

b. *Если произведение нескольких сомножителей делится на p, то, по крайней мере, один из сомножителей делится на p.*

Действительно (a), каждый сомножитель или взаимно прост с p, или же делится на p. Если бы все сомножители были взаимно просты с p, то и их произведение (3, f, § 2) было бы взаимно просто с p; поэтому хоть один сомножитель делится на p.

c. *Всякое целое, большее единицы, разлагается на произведение простых сомножителей и притом единственным способом, если отвлечься от порядка следования сомножителей.*

Действительно, пусть a — целое, большее единицы; обозначая буквою p_1 его наименьший простой делитель, имеем $a = p_1 a_1$. Если $a_1 > 1$, то, обозначая буквою p_2 его наименьший простой делитель, имеем $a_1 = p_2 a_2$. Если $a_2 > 1$, то подобно этому находим $a_2 = p_3 a_3$ и т. д., пока не придём к какому-либо a_n, равному единице. Тогда $a_{n-1} = p_n$. Перемножая все найденные равенства и производя сокращение, получим следующее разложение a на простые сомножители:

$$a = p_1 p_2 \cdots p_n.$$

Допустим, что для того же самого a существует и второе разложение на простые сомножители $a = q_1 q_2 \cdots q_s$. Тогда

$$p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_s.$$

Правая часть этого равенства делится на q_1. Следовательно (b), по крайней мере, один из сомножителей левой части должен делиться на q_1. Пусть, например, p_1 делится на q_1 (порядок нумерации сомножителей в нашем распоряжении); тогда $p_1 = q_1$ (p_1 кроме 1 делится только на p_1). Сокращая обе части равенства на $p_1 = q_1$, имеем $p_2 p_3 \cdots p_n = q_2 q_3 \cdots q_s$. Повторяя прежнее рассуждение применительно к этому равенству, получим $p_2 \cdots p_n = q_2 \cdots q_s$ и т. д., пока, наконец, в одной части равенства, например в левой, не сократятся все сомножители. Но одновременно должны сократиться и все сомножители правой части, так как равенство $1 = q_{n+1} \cdots q_s$ при $q_{n+1}, \ldots, q_s$, превосходящих 1, невозможно.

Таким образом, второе разложение на простые сомножители тождественно первому.

d. В разложении числа a на простые сомножители некоторые из них могут повторяться. Обозначая буквами $p_1, p_2, \ldots, p_k$ различные из них и буквами $\alpha_1, \alpha_2, \ldots, \alpha_k$ кратность их вхождения в a, получим так называемое *каноническое разложение числа a на сомножители*:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Пример. Каноническое разложение числа 588 000 будет: $588\,000 = 2^5 \cdot 3 \cdot 5^3 \cdot 7^2$.

c. *Пусть* $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ *— каноническое разложение числа* a. *Тогда все делители* a *суть все числа вида*

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}; \qquad 0 \leqslant \beta_1 \leqslant \alpha_1,\ 0 \leqslant \beta_2 \leqslant \alpha_2,\ \dots,\ 0 \leqslant \beta_k \leqslant \alpha_k. \tag{1}$$

Действительно, пусть d делит a. Тогда (b, § 1) $a = dq$ и, следовательно, все простые делители d входят в каноническое разложение a с показателями, не меньшими тех, с которыми они входят в каноническое разложение d. Поэтому d имеет вид (1).

Обратно, всякое d вида (1), очевидно, делит a.

Пример. Все делители числа $720 = 2^4 \cdot 3^2 \cdot 5$ получим, если в выражении $2^{\beta_1}3^{\beta_2}5^{\beta_3}$ заставим β_1, β_2, β_3 независимо друг от друга пробегать значения $\beta_1 = 0, 1, 2, 3, 4$; $\beta_2 = 0, 1, 2$; $\beta_3 = 0, 1$. Поэтому указанные делители будут: 1, 2, 4, 8, 16, 3, 6, 12, 24, 48, 9, 18, 36, 72, 144, 5, 10, 20, 40, 80, 15, 30, 60, 120, 240, 45, 90, 180, 360, 720.

Вопросы к главе I.

1. Пусть a и b — целые, не равные одновременно нулю, и $d = ax_0 + by_0$ — наименьшее положительное число вида $ax + by$ (x и y — целые). Доказать, что $d = (a, b)$. Отсюда вывести теорему 1, d, § 2 и теоремы e, § 2. Обобщить эти выводы, рассматривая числа вида $ax + by + \dots + fu$.

2. Доказать, что из всех рациональных дробей со знаменателями $\leqslant Q_s$ подходящая дробь $\frac{P_s}{Q_s}$ представляет число α наиболее точно.

3. Пусть вещественное число α разложено в непрерывную дробь, N — целое положительное, k — число его десятичных знаков, n — наибольшее целое с условием $Q_n \leqslant N$. Доказать, что $n \leqslant 5k + 1$. Для доказательства выражения для $Q_2, Q_3, Q_4, \dots, Q_n$ следует сравнить с теми, которые они имели бы, если бы все q_s были равны 1, и сравнить далее с числами $1, \xi, \xi^2, \dots, \xi^{n-1}$, где ξ — положительный корень уравнения $\xi^2 = \xi + 1$.

4. Пусть $\tau \geqslant 1$. Ряд расположенных в порядке возрастания рациональных несократимых дробей с положительными знаменателями, не превосходящими τ, называется *рядом Фарея, отвечающим* τ.

a. Доказать, что часть ряда Фарея, отвечающего τ, содержащая дроби α, с условием $0 \leqslant \alpha \leqslant 1$ может быть получена следующим способом: пишем дроби $\frac{0}{1}, \frac{1}{1}$. Если $2 \leqslant \tau$, то между этими дробями вставим ещё дробь $\frac{0+1}{1+1} = \frac{1}{2}$, затем в полученном ряде $\frac{0}{1}, \frac{1}{2}, \frac{1}{1}$ между каждыми двумя соседними дробями $\frac{a_1}{b_1}$ и $\frac{c_1}{d_1}$ с $b_1 + d_1 \leqslant \tau$ вставим дробь $\frac{a_1 + c_1}{b_1 + d_1}$ и т. д. до тех пор, пока это возможно. Предварительно доказать, что для любой пары соседних дробей $\frac{a}{b}$ и $\frac{c}{d}$ ряда, получаемого указанным способом, имеем $ad - bc = -1$.

b. Рассматривая ряд Фарея, доказать теорему: пусть $\tau \geqslant 1$, тогда всякое вещественное α можно представить в форме

$$\alpha = \frac{P}{Q} + \frac{\vartheta}{Q\tau}; \qquad 0 < Q \leqslant \tau,\ (P, Q) = 1, \quad |\vartheta| < 1.$$

c. Теорему вопроса b доказать, пользуясь h, § 4.

5, a. Доказать бесконечность числа простых чисел вида $4m + 3$.

b. Доказать бесконечность числа простых чисел вида $6m + 5$.

6. Доказать бесконечность числа простых чисел, подсчитывая число чисел, не превосходящих N, в каноническое разложение которых не входят простые числа, отличные от $p_1, p_2, \dots, p_k$.

7. Пусть K — целое положительное. Доказать, что в ряде натуральных чисел имеется бесчисленное множество последовательностей $M, M+1, \dots, M+K-1$, не содержащих простых чисел.

8. Доказать, что среди чисел, представляемых многочленом $a_0x^n + a_1x^{n-1} + \dots + a_n$, где $n > 0$, $a_0, a_1, \dots, a_n$ — целые и $a_0 > 0$, имеется бесчисленное множество составных.

9, a. Доказать, что неопределённому уравнению

$$x^2 + y^2 = z^2, \quad x > 0,\ y > 0,\ z > 0, \quad (x, y, z) = 1 \tag{1}$$

удовлетворяют те и только те системы x, y, z, где одно из чисел x и y имеет вид $2uv$, другое — вид $u^2 - v^2$, наконец, z имеет вид $u^2 + v^2$; при этом $u > v > 0$, $(u, v) = 1$, uv — чётное.

b. Пользуясь теоремой вопроса a, доказать неразрешимость в целых положительных x, y, z уравнения $x^4 + y^4 = z^2$.

10. Доказать теорему: если уравнение $x^n + a_1x^{n-1} + \dots + a_n = 0$, где $n > 0$ и $a_1, \dots, a_n$ — целые, имеет рациональный корень, то этот корень — целое число.

11, a. Пусть $S=\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n}$; $n>1$. Доказать, что S — не целое.

b. Пусть $S=\frac{1}{3}+\frac{1}{5}+\ldots+\frac{1}{2n+1}$; $n>0$. Доказать, что S — не целое.

12. Пусть n — целое, $n>0$. Доказать, что все коэффициенты разложения бинома Ньютона $(a+b)^n$ будут нечётными тогда и только тогда, когда n имеет вид $2^\alpha-1$.

Численные примеры к главе I.

1, a. Применяя алгоритм Эвклида, найти (6188, 4709).

b. Найти (81 719, 52 003, 33 649, 30 107).

2, a. Разложив в непрерывную дробь $\alpha=\frac{125}{92}$ и составив таблицу подходящих дробей (d, § 4), найти: α) δ_4, β) представление α в форме, указанной в вопросе 4, b, считая $\tau=20$.

b. Разложив в непрерывную дробь $\alpha=\frac{5391}{3976}$ и составив таблицу подходящих дробей, найти: α) δ_6, β) представление α в форме, указанной в вопросе 4, b, считая $\tau=1000$.

3. Составить ряд дробей Фарея (вопрос 4) от 0 до 1, исключая 1, со знаменателями, не превосходящими 8.

4. Составить таблицу простых чисел, меньших 100.

5, a. Найти каноническое разложение числа 82 798 848.

b. Найти каноническое разложение числа 81 057 226 635 000.

ГЛАВА ВТОРАЯ.

ВАЖНЕЙШИЕ ФУНКЦИИ, ВСТРЕЧАЮЩИЕСЯ В ТЕОРИИ ЧИСЕЛ.

§ 1. Функции $[x]$, $\{x\}$.

a. Важную роль в теории чисел играет функция $[x]$; она определяется для всех вещественных x и представляет собою наибольшее целое, не превосходящее x. Эта функция называется *целой частью от* x.

Примеры.

$$[7]=7;\quad [2{,}6]=2;\quad [-4{,}75]=-5.$$

Иногда рассматривается также функция $\{x\}=x-[x]$. Эта функция называется *дробной частью от* x.

Примеры.

$$\{7\}=0;\quad \{2{,}6\}=0{,}6;\quad \{-4{,}75\}=0{,}25.$$

b. Чтобы показать пользу введённых нами функций, докажем теорему:

Показатель, с которым данное простое p входит в произведение $n!$, равен

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\ldots$$

Действительно, число сомножителей произведения $n!$, кратных p, будет $\left[\frac{n}{p}\right]$, из них кратных p^2 будет $\left[\frac{n}{p^2}\right]$; из этих последних кратных p^3 будет $\left[\frac{n}{p^3}\right]$ и т. д. Сумма указанных чисел и даст искомый показатель, так как каждый сомножитель произведения $n!$, кратный

p^m, но не p^{m+1}, считается указанным путём m раз, как кратный p, p^2, p^3, ..., наконец, p^m.

Пример. Показатель, с которым число 3 входит в произведение 40!, будет следующий:

$$\left[\frac{40}{3}\right]+\left[\frac{40}{9}\right]+\left[\frac{40}{27}\right]=13+4+1=18.$$

§ 2. Суммы, распространённые на делители числа.

a. Особенно важную роль в теории чисел играют мультипликативные функции. Функция $\vartheta(a)$ называется *мультипликативной*, если выполнены следующие условия:

1. *Функция $\vartheta(a)$ определена для всех целых положительных a и не обращается в нуль хотя бы при одном таком a.*

2. *Для любых положительных взаимно простых a_1 и a_2 имеем*

$$\vartheta(a_1a_2)=\vartheta(a_1)\vartheta(a_2).$$

Пример. Нетрудно видеть, что мультипликативной будет функция $\vartheta(a)=a^s$, где s — любое вещественное, или комплексное, число.

b. Из указанных свойств функции $\vartheta(a)$, в частности, следует, что $\vartheta(1)=1$. Действительно, пусть $\vartheta(a_0)$ не равно нулю, тогда $\vartheta(a_0)=\vartheta(1\cdot a_0)=\vartheta(1)\vartheta(a_0)$, т. е. $\vartheta(1)=1$. Кроме того, получается следующее важное свойство: если $\vartheta_1(a)$ и $\vartheta_2(a)$ — функции мультипликативные, то и $\vartheta_0(a)=\vartheta_1(a)\vartheta_2(a)$ — также функция мультипликативная. Действительно, находим

$$\vartheta_0(1)=\vartheta_1(1)\vartheta_2(1)=1.$$

Кроме того, при $(a_1, a_2)=1$ находим

$$\vartheta_0(a_1a_2)=\vartheta_1(a_1a_2)\vartheta_2(a_1a_2)=\vartheta_1(a_1)\vartheta_1(a_2)\vartheta_2(a_1)\vartheta_2(a_2)=$$
$$=\vartheta_1(a_1)\vartheta_2(a_1)\vartheta_1(a_2)\vartheta_2(a_2)=\vartheta_0(a_1)\vartheta_0(a_2).$$

c. *Пусть $\vartheta(a)$ — мультипликативная функция и $a=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$ — каноническое разложение числа a. Тогда, обозначая символом $\sum_{d\mid a}$ сумму, распространённую на*

все делители d числа a, имеем

$$\sum_{d\mid a}\vartheta(d)=(1+\vartheta(p_1)+\vartheta(p_1^2)+\dots+\vartheta(p_1^{\alpha_1}))\dots$$
$$\dots(1+\vartheta(p_k)+\vartheta(p_k^2)+\dots+\vartheta(p_k^{\alpha_k}))$$

(*в случае $a=1$ правую часть считаем равной* 1).

Чтобы доказать это тождество, раскроем скобки в правой части. Тогда получим сумму слагаемых вида

$$\vartheta(p_1^{\beta_1})\vartheta(p_2^{\beta_2})\dots\vartheta(p_k^{\beta_k})=\vartheta(p_1^{\beta_1}p_2^{\beta_2}\dots p_k^{\beta_k});$$

$$0\leqslant\beta_1\leqslant\alpha_1,\ 0\leqslant\beta_2\leqslant\alpha_2,\ \dots,\ 0\leqslant\beta_k\leqslant\alpha_k,$$

причём ни одно такое слагаемое не будет пропущено и не повторится более одного раза, а это (**c, § 6, гл. I**) как раз будет то, что стоит в левой части.

d. При $\vartheta(a)=a^s$ тождество **c** примет вид

$$\sum_{d\mid a}d^s=(1+p_1^s+p_1^{2s}+\dots+p_1^{\alpha_1 s})\dots$$
$$\dots(1+p_k^s+p_k^{2s}+\dots+p_k^{\alpha_k s}). \qquad (1)$$

В частности, при $s=1$ левая часть (1) представит *сумму делителей* $S(a)$ числа a. Упрощая правую часть, получим

$$S(a)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\dots\frac{p_k^{\alpha_k+1}-1}{p_k-1}.$$

Пример.

$$S(720)=S(2^4\cdot3^2\cdot5)=\frac{2^{4+1}-1}{2-1}\cdot\frac{3^{2+1}-1}{3-1}\cdot\frac{5^{1+1}-1}{5-1}=2418.$$

При $s=0$ левая часть (1) представит *число делителей* $\tau(a)$ числа a, и мы получим

$$\tau(a)=(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1).$$

Пример.

$$\tau(720)=(4+1)(2+1)(1+1)=30.$$

§ 3. Функция Мёбиуса.

a. *Функция Мёбиуса* $\mu(a)$ определяется для всех целых положительных a. Она задаётся равенствами: $\mu(a)=0$, если a делится на квадрат, отличный от единицы; $\mu(a)=(-1)^k$, если a не делится на квадрат, отличный от единицы, при этом k обозначает число простых делителей числа a; в частности, при $a=1$ считаем $k=0$, поэтому принимаем $\mu(1)=1$.

Примеры.

$$\begin{array}{lll}\mu(1)=1, & \mu(5)=-1, & \mu(9)=0,\\ \mu(2)=-1, & \mu(6)=1, & \mu(10)=1,\\ \mu(3)=-1, & \mu(7)=-1, & \mu(11)=-1,\\ \mu(4)=0, & \mu(8)=0, & \mu(12)=0.\end{array}$$

b. *Пусть* $\vartheta(a)$ — *мультипликативная функция и*

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$$

— *каноническое разложение числа* a. *Тогда*

$$\sum_{d\mid a}\mu(d)\vartheta(d)=(1-\vartheta(p_1))(1-\vartheta(p_2))\dots(1-\vartheta(p_k)).$$

(*В случае* $a=1$ *правую часть считаем равной* 1.)

Действительно, функция $\mu(a)$, очевидно, мультипликативная. Поэтому мультипликативной будет и функция $\vartheta_1(a)=\mu(a)\vartheta(a)$. Применяя к последней тождество c, § 2 и имея в виду, что $\vartheta_1(p)=-\vartheta(p)$; $\vartheta_1(p^s)=0$ при $s>1$, мы и убедимся в справедливости нашей теоремы.

c. В частности, полагая $\vartheta(a)=1$, из b получим

$$\sum_{d\mid a}\mu(d)\begin{cases}=0, & \text{если } a>1,\\ =1, & \text{если } a=1.\end{cases}$$

Полагая же $\vartheta(d)=\frac{1}{d}$, получим

$$\sum_{d\mid a}\frac{\mu(d)}{d}\begin{cases}=\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_k}\right), & \text{если } a>1,\\ =1, & \text{если } a=1.\end{cases}$$

d. *Пусть целым положительным*

$$\delta=\delta_1,\ \delta_2,\ \dots,\ \delta_n$$

отвечают любые вещественные или комплексные $f=f_1,\ f_2,\ \dots,\ f_n$. *Тогда, обозначая символом* S' *сумму значений* f, *отвечающих значениям* δ, *равным* 1, *и символом* S_d *сумму значений* f, *отвечающих значениям* δ, *кратным* d, *будем иметь*

$$S'=\sum\mu(d)S_d,$$

где d *пробегает все целые положительные числа, делящие хоть одно значение* δ.

Действительно, ввиду c имеем

$$S'=f_1\sum_{d\mid\delta_1}\mu(d)+f_2\sum_{d\mid\delta_2}\mu(d)+\dots+f_n\sum_{d\mid\delta_n}\mu(d).$$

Собирая же вместе члены с одним и тем же значением d и вынося при этом $\mu(d)$ за скобки, в скобках получим сумму тех и только тех f, у которых соответствующие им δ кратны d, а это и есть S_d.

§ 4. Функция Эйлера.

a. *Функция Эйлера* $\varphi(a)$ определяется для всех целых положительных a и представляет собою число чисел ряда

$$0,\ 1,\ \dots,\ a-1 \tag{1}$$

взаимно простых с a.

Примеры.

$$\begin{array}{ll}\varphi(1)=1, & \varphi(4)=2,\\ \varphi(2)=1, & \varphi(5)=4,\\ \varphi(3)=2, & \varphi(6)=2.\end{array}$$

b. *Пусть*

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k} \tag{2}$$

— *каноническое разложение числа* a. *Тогда*

$$\varphi(a)=a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_k}\right). \tag{3}$$

или также

$$\varphi(a) = (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1}) \dots (p_k^{\alpha_k} - p_k^{\alpha_k-1}); \quad (4)$$

в частности,

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}, \quad \varphi(p) = p - 1. \quad (5)$$

Действительно, применим теорему d, § 3. При этом числа δ и числа f определим так: пусть x пробегает числа ряда (1); каждому значению x приведём в соответствие число $\delta = (x, a)$ и число $f = 1$.

Тогда S' обратится в число значений $\delta = (x, a)$, равных 1, т. е. в $\varphi(a)$. А S_d обратится в число значений $\delta = (x, a)$, кратных d. Но (x, a) может быть кратным d лишь при условии, что d — делитель числа a. При наличии же этого условия S_d обратится в число значений x, кратных d, т. е. в $\frac{a}{d}$. И мы получим

$$\varphi(a) = \sum_{d \backslash a} \mu(d) \frac{a}{d},$$

откуда ввиду **c**, § 3 следует формула (3), а из последней ввиду (2) следует формула (4).

Примеры.

$$\varphi(60) = 60\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 16;$$

$$\varphi(81) = 81 - 27 = 54;$$

$$\varphi(5) = 5 - 1 = 4.$$

c. *Функция $\varphi(a)$ есть функция мультипликативная.* Действительно, при $(a_1, a_2) = 1$ из **b**, очевидно, следует

$$\varphi(a_1, a_2) = \varphi(a_1)\varphi(a_2).$$

Пример. $\varphi(405) = \varphi(81)\varphi(5) = 54 \cdot 4 = 216$.

d. $\sum_{d \backslash a} \varphi(d) = a$.

В справедливости этой формулы убедимся, применяя тождество **c**, § 2, которое при $\theta(a) = \varphi(a)$ даёт

$$\sum_{d \backslash a} \varphi(d) = (1 + \varphi(p_1) + \varphi(p_1^2) + \dots + \varphi(p_1^{\alpha_1})) \dots$$

$$\dots (1 + \varphi(p_k) + \varphi(p_k^2) + \dots + \varphi(p_k^{\alpha_k})).$$

Ввиду (5) правая часть перепишется так:

$$(1 + (p_1 - 1) + (p_1^2 - p_1) + \dots + (p_1^{\alpha_1} - p_1^{\alpha_1-1})) \dots$$

$$\dots (1 + (p_k - 1) + (p_k^2 - p_k) + \dots + (p_k^{\alpha_k} - p_k^{\alpha_k-1})),$$

что после приведения в каждой большой скобке подобных членов окажется равным $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = a$.

Пример. Полагая $a = 12$, находим

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) =$$
$$= 1 + 1 + 2 + 2 + 2 + 4 = 12.$$

Вопросы к главе II.

1. **a.** Пусть в интервале $Q \leqslant x \leqslant R$ функция $f(x)$ непрерывна и неотрицательна. Доказать, что сумма

$$\sum_{Q < x \leqslant R} [f(x)]$$

выражает число целых точек (точек с целыми координатами) плоской области: $Q < x \leqslant R$, $0 < y \leqslant f(x)$.

b. Пусть P и Q — положительные нечётные взаимно простые. Доказать, что

$$\sum_{0 < x < \frac{Q}{2}} \left[\frac{P}{Q} x\right] + \sum_{0 < y < \frac{P}{2}} \left[\frac{Q}{P} y\right] = \frac{P-1}{2} \cdot \frac{Q-1}{2}$$

c. Пусть $r > 0$ и T — число целых точек области $x^2 + y^2 \leqslant r^2$. Доказать, что

$$T = 1 + 4[r] + 8 \sum_{0 < x \leqslant \frac{r}{\sqrt{2}}} [\sqrt{r^2 - x^2}] - 4\left[\frac{r}{\sqrt{2}}\right]^2.$$

d. Пусть $n>0$ и T — число целых точек области $x>0$, $y>0$, $xy\leqslant n$. Доказать, что

$$T=2\sum_{0<x\leqslant\sqrt{n}}\left[\frac{n}{x}\right]-[\sqrt{n}]^2.$$

2. Пусть $n>0$, m — целое, $m>1$ и x пробегает целые положительные числа, не делящиеся на m-ю степень целого, превосходящего 1. Доказать, что

$$\sum_x\left[\sqrt[m]{\frac{n}{x}}\right]=[n].$$

3. Пусть положительные α и β таковы, что

$$[\alpha x];\quad x=1,\ 2,\ \ldots;\ [\beta y];\ y=1,\ 2,\ \ldots$$

образуют, вместе взятые, все числа натурального ряда без повторений. Доказать, что это имеет место тогда и только тогда, когда α иррациональное, причём

$$\frac{1}{\alpha}+\frac{1}{\beta}=1.$$

4, **a.** Пусть $\tau\geqslant 1$, $t=[\tau]$ и $x_1,\ x_2,\ \ldots,\ x_t$ — числа $1,\ 2,\ \ldots,\ t$, расположенные в таком порядке, чтобы числа

$$0,\quad \{\alpha x_1\},\quad \{\alpha x_2\},\ \ldots,\ \{\alpha x_t\},\quad 1$$

шли не убывая. Доказать теорему вопроса 4, **b**, гл. I, рассматривая разности соседних чисел последнего ряда.

b. Пусть $X,\ Y,\ \ldots,\ Z$ — вещественные числа, каждое из которых не меньше 1; $\alpha,\ \beta,\ \ldots,\ \gamma$ — вещественные. Доказать, что существуют целые $x,\ y,\ \ldots,\ z$, не равные одновременно нулю, и целое u, удовлетворяющие условиям:

$$|x|\leqslant X,\quad |y|\leqslant Y,\ \ldots,\ |z|\leqslant Z,$$

$$(x,\ y,\ \ldots,\ z)=1,\quad |\alpha x+\beta y+\ldots+\gamma z-u|<\frac{1}{XY\ldots Z}.$$

5. Пусть α — вещественное, c — целое, $c>0$. Доказать, что

$$\left[\frac{[\alpha]}{c}\right]=\left[\frac{\alpha}{c}\right].$$

6, **a.** Пусть $\alpha,\ \beta,\ \ldots,\ \lambda$ — вещественные. Доказать, что

$$[\alpha+\beta+\ldots+\lambda]\geqslant[\alpha]+[\beta]+\ldots+[\lambda].$$

b. Пусть $a,\ b,\ \ldots,\ l$ — целые положительные, $a+b+\ldots+l=n$. Применяя **b**, § 1, доказать, что

$$\frac{n!}{a!b!\ldots l!}$$

есть целое число.

7. Пусть h — целое, $h>0$, p — простое и

$$u_s=\frac{p^{s+1}-1}{p-1}.$$

Представляя h в форме $h=p_mu_m+p_{m-1}u_{m-1}+\ldots+p_1u_1+p_0$, где u_m — наибольшее u_s, не превосходящее h, p_mu_m — наибольшее кратное u_m, не превосходящее h, $p_{m-1}u_{m-1}$ — наибольшее кратное u_{m-1}, не превосходящее $h-p_mu_m$, $p_{m-2}u_{m-2}$ — наибольшее кратное u_{m-2}, не превосходящее $h-p_mu_m-p_{m-1}u_{m-1}$ и т. д., доказать, что числа a с условием, что в каноническое разложение $a!$ число p входит с показателем h, существуют тогда и только тогда, когда все $p_m,\ p_{m-1},\ \ldots,\ p_1,\ p_0$ меньше p, причём в этом случае указанные a суть все числа вида

$$a=p_mp^{m+1}+p_{m-1}p^m+\ldots+p_1p^2+p_0p+p',$$

где p' имеет значения: $0,\ 1,\ \ldots,\ p-1$.

8, **a.** Пусть в интервале $Q\leqslant x\leqslant R$ функция $f(x)$ имеет вторую непрерывную производную. Полагая

$$\rho(x)=\frac{1}{2}-\{x\},\quad \sigma(x)=\int_0^x\rho(z)\,dz,$$

доказать, что (формула Сонина)

$$\sum_{Q<x\leqslant R}f(x)=\int_Q^R f(x)\,dx+\rho(R)f(R)-\rho(Q)f(Q)-\sigma(R)f'(R)+$$

$$+\sigma(Q)f'(Q)+\int_Q^R\sigma(x)f''(x)\,dx.$$

b. Пусть условие вопроса **a** выполняется при сколь угодно больших R, причём $\int_Q^\infty|f''(x)|\,dx$ сходится. Доказать, что

$$\sum_{Q<x\leqslant R}f(x)=$$

$$=C+\int^R f(x)\,dx+\rho(R)f(R)-\sigma(R)f'(R)-\int_R^\infty\sigma(x)f''(x)\,dx,$$

где C не зависит от R.

c. Если B принимает лишь положительные значения и отношение $\frac{|A|}{B}$ остаётся ограниченным сверху, то пишем $A=O(B)$.

Пусть n—целое, $n > 1$. Доказать, что

$$\ln(n!) = n\ln n - n + O(\ln n).$$

9, a. Пусть $n \geqslant 2$, $\Theta(z, z_0) = \sum_{z_0 < p \leqslant z} \ln p$, где p пробегает простые числа. Пусть, далее, $\Theta(z) = \Theta(z, 0)$ и при $x > 0$

$$\psi(x) = \Theta(x) + \Theta(\sqrt{x}) + \Theta(\sqrt[3]{x}) + \ldots$$

Доказать, что

α) $\ln([n]!) = \psi(n) + \psi\left(\frac{n}{2}\right) + \psi\left(\frac{n}{3}\right) + \ldots$;

β) $\psi(n) < 2n$;

γ) $\Theta\left(n, \frac{n}{2}\right) + \Theta\left(\frac{n}{3}, \frac{n}{4}\right) + \Theta\left(\frac{n}{5}, \frac{n}{6}\right) + \ldots = n\ln 2 + O(\sqrt{n})$.

b. При $n > 2$ доказать, что

$$\sum_{p \leqslant n} \frac{\ln p}{p} = \ln n + O(1),$$

где p пробегает простые числа.

c. Пусть ε—произвольное положительное постоянное. Доказать, что в ряде натуральных чисел существует бесчисленное множество пар p_n, p_{n+1} простых чисел с условием

$$p_{n+1} < p_n(1 + \varepsilon).$$

d. Пусть $n > 2$. Доказать, что

$$\sum_{p \leqslant n} \frac{1}{p} = C + \ln\ln n + O\left(\frac{1}{\ln n}\right),$$

где p пробегает простые числа и C не зависит от n.

e. Пусть $n > 2$. Доказать, что

$$\prod_{p \leqslant n} \left(1 - \frac{1}{p}\right) = \frac{C_0}{\ln n}\left(1 + O\left(\frac{1}{\ln n}\right)\right),$$

где p пробегает простые числа и C_0 не зависит от n.

10, a. Пусть $\theta(a)$—функция мультипликативная. Доказать, что $\theta_1(a) = \sum_{d \mid a} \theta(d)$—также функция мультипликативная.

b. Пусть функция $\theta(a)$ определена для всех целых положительных a и функция $\varphi(a) = \sum_{d \mid a} \theta(a)$ мультипликативная. Доказать, что функция $\theta(a)$ также мультипликативная.

11. Пусть при $m > 0$ $\tau_m(a)$ обозначает число решений неопределённого уравнения $x_1 x_2 \ldots x_m = a$ ($x_1, x_2, \ldots, x_m$ независимо друг от друга пробегают целые положительные числа); в частности, очевидно, $\tau_1(a) = 1$, $\tau_2(a) = \tau(a)$. Доказать, что

a. $\tau_m(a)$—функция мультипликативная.

b. Если каноническое разложение числа a имеет вид

$$a = p_1 p_2 \ldots p_k, \quad \text{то } \tau_m(a) = m^k.$$

c. Если ε произвольное положительное постоянное, то

$$\lim_{a \to \infty} \frac{\tau_m(a)}{a^\varepsilon} = 0.$$

d. $\sum_{0 < a \leqslant n} \tau_m(a)$ выражает число решений неравенства $x_1 x_2 \ldots x_m \leqslant n$ в целых положительных $x_1, x_2, \ldots, x_m$.

12. Пусть $R(s)$ обозначает вещественную часть числа s.

При $R(s) > 1$ полагаем $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. Пусть $m > 0$, m—целое. Доказать, что

$$(\zeta(s))^m = \sum_{n=1}^{\infty} \frac{\tau_m(n)}{n^s}.$$

13, a. При $R(s) > 1$ доказать, что

$$\zeta(s) = \prod \frac{1}{1 - \frac{1}{p^s}},$$

где p пробегает все простые числа.

b. Доказать бесконечность числа простых чисел, исходя из того, что гармонический ряд—расходящийся.

c. Доказать бесконечность числа простых чисел, исходя из того, что $\zeta(2) = \frac{\pi^2}{6}$—число иррациональное.

14. Пусть $\Lambda(a) = \ln p$ для $a = p^l$, где p—простое и l—целое положительное; $\Lambda(a) = 0$ для других целых положительных a.

При $R(s) > 1$ доказать, что

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

15. Пусть $R(s) > 1$. Доказать, что

$$\prod_p \left(1 - \frac{1}{p^s}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s},$$

где p пробегает простые числа.

16, a. Пусть $n \geqslant 1$. Применяя d, § 3, доказать, что

$$1 = \sum_{0<d\leqslant n} \mu(d) \left[\frac{n}{d}\right].$$

b. Пусть $M(z, z_0) = \sum_{z_1<a\leqslant z} \mu(a)$; $M(x) = M(x, 0)$.

Доказать, что

a) $M(n) + M\left(\frac{n}{2}\right) + M\left(\frac{n}{3}\right) + \ldots = 1, \qquad n \geqslant 1.$

3) $M\left(n, \frac{n}{2}\right) + M\left(\frac{n}{3}, \frac{n}{4}\right) + M\left(\frac{n}{5}, \frac{n}{6}\right) + \ldots = -1, \qquad n \geqslant 2.$

c. Пусть $n \geqslant 1$, l — целое, $l > 1$, $T_{l,n}$ — число целых x с условием $0 < x \leqslant n$, не делящихся на l-ю степень целого, превосходящего 1. Применяя d, § 3, доказать, что

$$T_{l,n} = \sum_{d=1}^{\infty} \mu(d) \left[\frac{n}{d^l}\right].$$

17, a. Пусть a — целое, $a > 0$, и для целых $x_1, x_2, \ldots, x_n$ однозначно определена функция $f(x)$. Доказать, что

$$S' = \sum_{d \setminus a} \mu(d) S_d,$$

где S' обозначает сумму значений $f(x)$, распространённую на значения x, взаимно простые с a, и S_d — сумму значений $f(x)$, распространённую на значения x, кратные d.

b. Пусть $k > 1$ и заданы системы

$$x_1', x_2', \ldots, x_k'; x_1'', x_2'', \ldots, x_k''; \ldots; x_1^{(n)}, x_2^{(n)}, \ldots, x_k^{(n)},$$

каждая из которых состоит из целых чисел, не равных одновременно нулю. Пусть далее для этих систем однозначно определена функция $f(x_1, x_2, \ldots, x_k)$. Доказать, что

$$S' = \sum \mu(d) S_d,$$

где S' обозначает сумму значений $f(x_1, x_2, \ldots, x_k)$, распространённую на системы взаимно простых чисел, и S_d обозначает сумму значений $f(x_1, x_2, \ldots, x_k)$, распространённую на системы чисел, одновременно кратных d. При этом d пробегает целые положительные числа.

c. Пусть a — целое, $a > 0$, и для делителей δ числа a однозначно определена функция $F(\delta)$. Полагая

$$G(\delta) = \sum_{d \setminus \delta} F(d),$$

доказать, что (закон обращения числовых функций)

$$F(a) = \sum_{d \setminus a} \mu(d)\, G\left(\frac{a}{d}\right).$$

d. Пусть целым положительным

$$\delta_1, \delta_2, \ldots, \delta_n$$

отвечают любые вещественные, или комплексные, не равные нулю:

$$f_1, f_2, \ldots, f_n.$$

Доказать, что

$$P' = \prod P_d^{\mu(d)},$$

где P' обозначает произведение значений f, отвечающих значениям δ, равным 1, P_d обозначает произведение значений f, отвечающих значениям δ, кратным d, причём d пробегает все целые положительные числа, делящие хотя бы одно δ.

18. Пусть a — целое, $a > 1$, $\sigma_m(n) = 1^m + 2^m + \ldots + n^m$, $\psi_m(a)$ — сумма m-х степеней чисел ряда 1, 2, ..., a, взаимно простых с a; $p_1, p_2, \ldots, p_k$ — все простые делители числа a.

a. Применяя теорему вопроса 17, a, доказать, что

$$\psi_m(a) = \sum_{d \setminus a} \mu(d)\, d^m \sigma_m\left(\frac{a}{d}\right).$$

b. Доказать, что

$$\psi_1(a) = \frac{a}{2} \varphi(a).$$

c. Доказать, что

$$\psi_2(a)=\left(\frac{a^2}{3}+\frac{(-1)^k}{6}p_1p_2\dots p_k\right)\varphi(a).$$

19. Пусть $z>1$, a — целое, $a>0$, T_z — число чисел x с условиями $0<x\leqslant z$, $(x,\ a)=1$, ε — произвольное положительное постоянное.

a. Доказать, что

$$T_z=\sum_{d\mid a}\mu(d)\left[\frac{z}{d}\right].$$

b. Доказать, что

$$T_z=\frac{z}{a}\varphi(a)+O(a^\varepsilon).$$

c. Пусть $z>1$, $\pi(z)$ — число простых чисел, не превосходящих z, a — произведение простых чисел, не превосходящих $\sqrt{z}$. Доказать, что

$$\pi(z)=\pi(\sqrt{z})-1+\sum_{d\mid a}\mu(d)\left[\frac{z}{d}\right].$$

20. Пусть $R(s)>1$, a — целое, $a>0$. Доказать, что

$$\sum{}'\frac{1}{n^s}=\zeta(s)\prod\left(1-\frac{1}{p^s}\right),$$

где в левой части n пробегает целые положительные числа, взаимно простые с a, а в правой части p пробегает все простые делители числа a.

21, a. Вероятность P того, что k целых положительных чисел $x_1, x_2, \dots, x_k$ будут взаимно простыми, определим как предел при $N\to\infty$ вероятности P_N того, что будут взаимно простыми k чисел $x_1, x_2, \dots, x_k$, каждому из которых независимо от остальных присвоено одно из значений $1, 2, \dots, N$, принимаемых за равновозможные. Применяя теорему вопроса 17, b, доказать, что $P=(\zeta(k))^{-1}$.

b. Определяя вероятность P несократимости дроби $\frac{x}{y}$ аналогично тому, как в вопросе a при $k=2$, доказать, что

$$P=\frac{6}{\pi^2}.$$

22, a. Пусть $r\geqslant 2$ и T — число целых точек (x, y) с взаимно простыми координатами, лежащих в области $x^2+y^2\leqslant r^2$. Доказать, что

$$T=\frac{6}{\pi}r^2+O(r\ln r).$$

b. Пусть $r\geqslant 2$ и T — число целых точек (x, y, z) с взаимно простыми координатами, лежащих в области $x^2+y^2+z^2\leqslant r^2$. Доказать, что

$$T=\frac{4\pi}{3\zeta(3)}+O(r^2).$$

23, a. Первую теорему c, § 3 доказать, считая делители числа a, не делящиеся на квадрат целого, превосходящего 1, и имеющие $1, 2, \dots$ простых делителей.

b. Пусть a — целое, $a>1$, d пробегает делители числа a, имеющие не более чем m простых делителей; доказать, что при m чётном $\sum\mu(d)\geqslant 0$, а при m нечётном $\sum\mu(d)\leqslant 0$.

c. При условиях теоремы d, § 3, считая все f неотрицательными и заставляя d пробегать лишь числа, имеющие не более чем m простых делителей, доказать, что

$$S'\leqslant\sum\mu(d)S_d,\quad S'\geqslant\sum\mu(d)S_d$$

в зависимости от того, будет ли m чётное или нечётное.

d. Такие же, как в вопросе c, неравенства доказать при условиях вопроса 17, a, считая все значения $f(x)$ неотрицательными, а также при условиях 17, b, считая все значения $f(x_1, x_2, \dots, x_k)$ неотрицательными.

24. Пусть ε — любое постоянное с условиями $0<\varepsilon<\frac{1}{6}$, $N\geqslant 2$, $r=\ln N$, $0<q\leqslant N^{1-\varepsilon}$, $0\leqslant l<q$, $(q,\ l)=1$, $\pi(N, q, l)$ — число простых чисел с условиями: $p\leqslant N$, $p=qt+l$, где t — целое. Доказать, что

$$\pi(N, q, l)=O(\Delta);\quad \Delta=\frac{N(qr)^\varepsilon}{qr}.$$

Для доказательства, полагая $h=r^{1-\varepsilon}$, простые числа с указанными условиями следует рассматривать как частный случай всех чисел с этими условиями взаимно простых с a, где a — произведение всех простых, не превосходящих e^h и не делящих q. Следует применить теорему вопроса 23, d (условия вопроса 17, a) с указанным a и $m=2[2\ln r+1]$.

25. Пусть k — чётное, $k>0$, каноническое разложение числа a имеет вид $a=p_1p_2\dots p_k$ и d пробегает делители числа a с условием $0<d<\sqrt{a}$. Доказать, что

$$\sum_d\mu(d)=0.$$

26. Пусть k — целое, $k > 0$, d пробегает числа с условием $d > 0$, $\varphi(d) = k$. Доказать, что

$$\sum_d \mu(d) = 0.$$

27. Пользуясь выражением для $\varphi(a)$, доказать бесконечность числа простых чисел.

28, a. Теорему d, § 4 доказать, установив, что число чисел ряда $1, 2, \ldots, a$, имеющих с a один и тот же общий наибольший делитель δ, равно $\varphi\left(\frac{a}{\delta}\right)$.

b. Вывести выражение для $\varphi(a)$:
α) пользуясь теоремой вопроса 10, b;
β) пользуясь теоремой вопроса 17, c.

29. Пусть $R(s) > 2$. Доказать, что

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}.$$

30. Пусть n — целое, $n \geqslant 2$. Доказать, что

$$\sum_{m=1}^{n} \varphi(m) = \frac{3}{\pi^2} n^2 + O(n \ln n).$$

Численные примеры к главе II.

1, a. Найти показатель, с которым 5 входит в каноническое разложение 5258! (см. вопрос 5).

b. Найти каноническое разложение числа 125!

2, a. Найти $\tau(5600)$ и $S(5600)$.

b. Найти $\tau(116\,424)$ и $S(116\,424)$.

3. Составить таблицу значений функции $\mu(a)$ для всех $a = 1, 2, \ldots, 100$.

4. Найти α) $\varphi(5040)$, β) $\varphi(1\,294\,700)$.

5. Составить таблицу значений функции $\varphi(a)$ для всех $a = 1, 2, \ldots, 50$, пользуясь только формулой (5), § 4 и теоремой c, § 4.

ГЛАВА ТРЕТЬЯ.

СРАВНЕНИЯ.

§ 1. Основные понятия.

a. Мы будем рассматривать целые числа в связи с остатками от деления их на данное целое положительное m, которое назовём *модулем*.

Каждому целому числу отвечает определённый остаток от деления его на m (c, § 1, гл. I); если двум целым a и b отвечает один и тот же остаток r, то они называются *равноостаточными* по модулю m или *сравнимыми* по модулю m.

b. Сравнимость чисел a и b по модулю m записывается так:

$$a \equiv b \pmod{m},$$

что читается: a сравнимо с b по модулю m.

c. *Сравнимость чисел a и b по модулю m равносильна:*

1. *Возможности представить a в форме $a = b + mt$, где t — целое.*

2. *Делимости $a - b$ на m.*

Действительно, из $a \equiv b \pmod{m}$ следует

$$a = mq + r, \quad b = mq_1 + r; \quad 0 \leqslant r < m,$$

откуда

$$a - b = m(q - q_1), \quad a = b + mt, \quad t = q - q_1.$$

Обратно, из $a = b + mt$, представляя b в форме

$$b = mq_1 + r, \quad 0 \leqslant r < m,$$

выведем

$$a = mq + r; \quad q = q_1 + t,$$

т. е.

$$a \equiv b \pmod m.$$

Поэтому верно утверждение 1.

Из 1 непосредственно следует утверждение 2.

§ 2. Свойства сравнений, подобные свойствам равенств.

a. *Два числа, сравнимые с третьим, сравнимы между собою.*

Следует из a, § 1.

b. *Сравнения можно почленно складывать.*

Действительно, пусть

$$a_1 \equiv b_1 \pmod m,\ a_2 \equiv b_2 \pmod m,\ \ldots,\ a_k \equiv b_k \pmod m. \quad (1)$$

Тогда (1, c, § 1)

$$a_1 = b_1 + mt_1,\ a_2 = b_2 + mt_2,\ \ldots,\ a_k = b_k + mt_k, \quad (2)$$

откуда

$$a_1 + a_2 + \ldots + a_k = b_1 + b_2 + \ldots + b_k + m(t_1 + t_2 + \ldots + t_k),$$

или (1, c, § 1)

$$a_1 + a_2 + \ldots + a_k \equiv b_1 + b_2 + \ldots + b_k \pmod m.$$

Слагаемое, стоящее в какой-либо части сравнения, можно переносить в другую часть, переменив знак на обратный.

Действительно, складывая сравнение $a + b \equiv c \pmod m$ с очевидным сравнением $-b \equiv -b \pmod m$, получим $a \equiv c - b \pmod m$.

К каждой части сравнения можно прибавить (или отнять от неё) любое число, кратное модуля.

Действительно, складывая сравнение $a \equiv b \pmod m$ с очевидным сравнением $mk \equiv 0 \pmod m$, получим $a + mk \equiv b \pmod m$.

c. *Сравнения можно почленно перемножать.*

Действительно, рассмотрим снова сравнения (1) и вытекающие из них равенства (2). Перемножая почленно равенства (2), получим

$$a_1 a_2 \ldots a_k = b_1 b_2 \ldots b_k + mN,$$

где N — целое. Следовательно (1, c, § 1),

$$a_1 a_2 \ldots a_k \equiv b_1 b_2 \ldots b_k \pmod m.$$

Обе части сравнения можно возвысить в одну и ту же степень.

Это следует из предыдущего утверждения.

Обе части сравнения можно умножить на одно и то же целое.

Действительно, перемножив сравнение $a \equiv b \pmod m$ с очевидным сравнением $k \equiv k \pmod m$, получим $ak \equiv bk \pmod m$.

d. Свойства b и c (сложение и умножение сравнений) обобщаются следующей теоремой.

Если в выражении целой рациональной функции с целыми коэффициентами $S = \sum A_{\alpha_1, \ldots, \alpha_k} x_1^{\alpha_1} \ldots x_k^{\alpha_k}$ заменим $A_{\alpha_1, \ldots, \alpha_k}$, $x_1, \ldots, x_k$ числами $B_{\alpha_1, \ldots, \alpha_k}$, $y_1, \ldots, y_k$, сравнимыми с прежними по модулю m, то новое выражение S будет сравнимо с прежним по модулю m.

Действительно, из

$$A_{\alpha_1, \ldots, \alpha_k} \equiv B_{\alpha_1, \ldots, \alpha_k} \pmod m,$$

$$x_1 \equiv y_1 \pmod m,\ \ldots,\ x_k \equiv y_k \pmod m$$

находим (c)

$$x_1^{\alpha_1} \equiv y_1^{\alpha_1} \pmod m,\ \ldots,\ x_k^{\alpha_k} \equiv y_k^{\alpha_k} \pmod m,$$

$$A_{\alpha_1, \ldots, \alpha_k} x_1^{\alpha_1} \ldots x_k^{\alpha_k} \equiv B_{\alpha_1, \ldots, \alpha_k}\, y_1^{\alpha_1} \ldots y_k^{\alpha_k} \pmod m,$$

откуда, суммируя, получим

$$\sum A_{\alpha_1, \ldots, \alpha_k} x_1^{\alpha_1} \ldots x_k^{\alpha_k} \equiv \sum B_{\alpha_1, \ldots, \alpha_k} y_1^{\alpha_1} \ldots y_k^{\alpha_k} \pmod m.$$

Если

$$a \equiv b \pmod m,\ a_1 \equiv b_1 \pmod m,\ \ldots,\ a_n \equiv b_n \pmod m,$$

$$x \equiv x_1 \pmod m,$$

то

$$ax^n + a_1x^{n-1} + \ldots + a_n \equiv bx^n + b_1x^{n-1} + \ldots + b_n \pmod m.$$

Это утверждение является частным случаем предыдущего.

c. *Обе части сравнения можно разделить на их общий делитель, если последний взаимно прост с модулем.*

Действительно, из $a \equiv b \pmod m$, $a = a_1d$, $b = b_1d$, $(d, m) = 1$ следует, что разность $a - b$, равная $(a_1 - b_1)d$, делится на m. Поэтому (2, f, § 2, гл. I) $a_1 - b_1$ делится на m, т. е. $a_1 \equiv b_1 \pmod m$.

§ 3. Дальнейшие свойства сравнений.

a. *Обе части сравнения и модуль можно умножить на одно и то же целое.*

Действительно, из $a \equiv b \pmod m$ следует

$$a = b + mt, \quad ak = bk + mkt$$

и, следовательно, $ak \equiv bk \pmod{mk}$.

b. *Обе части сравнения и модуль можно разделить на любой их общий делитель.*

Действительно, пусть

$$a \equiv b \pmod m, \quad a = a_1d, \quad b = b_1d, \quad m = m_1d.$$

Имеем

$$a = b + mt, \quad a_1d = b_1d + m_1dt, \quad a_1 = b_1 + m_1t$$

и, следовательно, $a_1 \equiv b_1 \pmod{m_1}$.

c. *Если сравнение $a \equiv b$ имеет место по нескольким модулям, то оно имеет место и по модулю, равному общему наименьшему кратному этих модулей.*

В самом деле, из $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ..., ..., $a \equiv b \pmod{m_k}$ следует, что разность $a - b$ делится на все модули $m_1, m_2, \ldots, m_k$. Поэтому (**c**, § 3, гл. **I**) она должна делиться и на общее наименьшее кратное m этих модулей, т. е. $a \equiv b \pmod m$.

d. *Если сравнение имеет место по модулю m, то оно имеет место и по модулю d, равному любому делителю числа m.*

В самом деле, из $a \equiv b \pmod m$ следует, что разность $a - b$ должна делиться на m; поэтому (1, b, § 1, гл. I) она должна делиться и на любой делитель d числа m, т. е. $a \equiv b \pmod d$.

e. *Если одна часть сравнения и модуль делятся на какое-либо число, то и другая часть сравнения должна делиться на то же число.*

Действительно, из $a \equiv b \pmod m$ следует $a = b + mt$, если a и m кратны d, то (2, b, § 1, гл. I) и b должно быть кратным d, что и утверждалось.

f. *Если $a \equiv b \pmod m$, то $(a, m) = (b, m)$.*

Действительно, ввиду 2, b, § 2, гл. I это равенство непосредственно следует из $a = b + mt$.

§ 4. Полная система вычетов.

a. Числа равноостаточные, или, что то же самое, сравнимые по модулю m, образуют *класс чисел по модулю m*.

Из такого определения следует, что всем числам класса отвечает один и тот же остаток r, и мы получим все числа класса, если в форме $mq + r$ заставим q пробегать все целые числа.

Соответственно m различным значениям r имеем m классов чисел по модулю m.

b. Любое число класса называется *вычетом по модулю m* по отношению ко всем числам того же класса. Вычет, получаемый при $q = 0$, равный самому остатку r, называется *наименьшим неотрицательным вычетом*.

Вычет ρ, самый малый по абсолютной величине, называется *абсолютно наименьшим вычетом*.

Очевидно при $r < \frac{m}{2}$ имеем $\rho = r$; при $r > \frac{m}{2}$ имеем $\rho = r - m$; наконец, если m чётное и $r = \frac{m}{2}$, то за ρ можно принять любое из двух чисел $\frac{m}{2}$ и $\frac{m}{2} - m = -\frac{m}{2}$.

Взяв от каждого класса по одному вычету, получим *полную систему вычетов по модулю m*. Чаще всего в

качестве полной системы вычетов употребляют наименьшие неотрицательные вычеты $0, 1, \ldots, m-1$ или также абсолютно наименьшие вычеты; последние, как это следует из вышеизложенного, в случае нечётного m представляются рядом

$$-\frac{m-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-1}{2},$$

а в случае чётного m каким-либо из двух рядов

$$-\frac{m}{2}+1, \ldots, -1, 0, 1, \ldots, \frac{m}{2},$$

$$-\frac{m}{2}, \ldots, -1, 0, 1, \ldots, \frac{m}{2}-1.$$

c. *Любые m чисел, попарно несравнимые по модулю m, образуют полную систему вычетов по этому модулю.*

Действительно, будучи несравнимы, эти числа тем самым принадлежат к различным классам, а так как их m, т. е. столько же, сколько и классов, то в каждый класс наверно попадёт по одному числу.

d. *Если $(a, m)=1$ и x пробегает полную систему вычетов по модулю m, то $ax+b$, где b — любое целое, тоже пробегает полную систему вычетов по модулю m.*

Действительно, чисел $ax+b$ будет столько же, сколько и чисел x, т. е. m. Согласно c остаётся, следовательно, только показать, что любые два числа ax_1+b и ax_2+b, отвечающие несравнимым x_1 и x_2, будут сами несравнимы по модулю m.

Но допустив, что $ax_1+b \equiv ax_2+b \pmod m$, мы придём к сравнению $ax_1 \equiv ax_2 \pmod m$, откуда, вследствие $(a, m)=1$, получим $x_1 \equiv x_2 \pmod m$, что противоречит предположению о несравнимости чисел x_1 и x_2.

§ 5. Приведённая система вычетов.

a. Согласно f, § 3 числа одного и того же класса по модулю m имеют с модулем один и тот же общий наибольший делитель. Особенно важны классы, для которых этот делитель равен единице, т. е. классы, содержащие числа, взаимно простые с модулем.

Взяв от каждого такого класса по одному вычету, получим *приведённую систему вычетов по модулю m*. Приведённую систему вычетов, следовательно, можно составить из чисел полной системы, взаимно простых с модулем. Обыкновенно приведённую систему вычетов выделяют из системы наименьших неотрицательных вычетов: $0, 1, \ldots, m-1$. Так как среди этих чисел число взаимно простых с m есть $\varphi(m)$, то число чисел приведённой системы, равно как и число классов, содержащих числа, взаимно простые с модулем, есть $\varphi(m)$.

Пример. Приведённая система вычетов по модулю 42 будет

$$1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41.$$

b. *Любые $\varphi(m)$ чисел, попарно несравнимые по модулю m и взаимно простые с модулем, образуют приведённую систему вычетов по модулю m.*

Действительно, будучи несравнимыми и взаимно простыми с модулем, эти числа тем самым принадлежат к различным классам, содержащим числа, взаимно простые с модулем, а так как их $\varphi(m)$, т. е. столько же, сколько и классов указанного вида, то в каждый класс наверно попадёт по одному числу.

c. *Если $(a, m)=1$ и x пробегает приведённую систему вычетов по модулю m, то ax тоже пробегает приведённую систему вычетов по модулю m.*

Действительно, чисел ax будет столько же, сколько и чисел x, т. е. $\varphi(m)$. Согласно b остаётся, следовательно, только показать, что числа ax по модулю m несравнимы и взаимно просты с модулем. Но первое доказано в d, § 4 для чисел более общего вида $ax+b$, второе же следует из $(a, m)=1$, $(x, m)=1$.

§ 6. Теоремы Эйлера и Ферма.

a. *При $m>1$ и $(a, m)=1$ имеем (теорема Эйлера):*

$$a^{\varphi(m)} \equiv 1 \pmod m.$$

Действительно, если x пробегает приведённую систему вычетов

$$x = r_1, r_2, \ldots, r_c;\ c = \varphi(m),$$

составленную из наименьших неотрицательных вычетов, то наименьшие неотрицательные вычеты $r_1, r_2, \ldots, r_c$ чисел ax будут пробегать ту же систему, но расположенную, вообще говоря, в ином порядке (c, § 5)

Перемножая почленно сравнения

$$ar_1 \equiv r_1 \pmod m, \quad ar_2 \equiv r_2 \pmod m, \quad \ldots, \quad ar_c \equiv r_c \pmod m,$$

получим

$$a^c r_1 r_2 \ldots r_c \equiv r_1 r_2 \ldots r_c \pmod m,$$

откуда, деля обе части на произведение $r_1 r_2 \ldots r_c = r_1 r_2 \ldots r_c$, получим

$$a^c \equiv 1 \pmod m.$$

b. *При p простом и a, не делящемся на p, имеем (теорема Ферма):*

$$a^{p-1} \equiv 1 \pmod p. \tag{1}$$

Эта теорема является следствием теоремы a при $m = p$. Последней теореме можно придать более удобную форму. Именно, умножая обе части сравнения (1) на a, получим сравнение

$$a^p \equiv a \pmod p,$$

справедливое уже при всех целых a, так как оно верно и при a, кратном p.

Вопросы к главе III.

1, a. Представляя целое число в обычной десятичной системе исчисления, вывести признаки делимости на 3, 9, 11.

b. Представляя целое число в системе исчисления с основанием 100, вывести признак делимости на 101.

c. Представляя целое число в системе исчисления с основанием 1000, вывести признаки делимости на 37, 7, 11, 13.

2, a. Пусть $m > 0$, $(a, m) = 1$, b — целое, x пробегает полную, а ξ — приведённую систему вычетов по модулю m. Доказать, что

$$\alpha) \quad \sum_x \left\{ \frac{ax+b}{m} \right\} = \frac{1}{2}(m-1),$$

$$\beta) \quad \sum_\xi \left\{ \frac{a\xi}{m} \right\} = \frac{1}{2}\varphi(m).$$

b. Пусть $m > 0$, $(a, m) = 1$; b, N, t — целые, $t > 0$, $f(x) = \frac{ax+b}{m}$, $f(N) > 0$, $f(N+mt) > 0$. Доказать, что для трапеции, ограниченной прямыми $x = N$, $x = N + mt$, $y = 0$, $y = f(x)$, имеем

$$S = \sum \delta, \tag{1}$$

где S — площадь трапеции, а сумма, стоящая справа, распространена на все целые точки трапеции, причём $\delta = 1$ для внутренних точек, $\delta = \frac{1}{4}$ для вершин, $\delta = \frac{1}{2}$ — для остальных точек контура.

c. Считая, в отличие от вопроса b, $\delta = \frac{1}{6}$ для вершин, формулу (1) доказать для треугольника с целыми вершинами.

3, a. Пусть $m > 0$, $(a, m) = 1$, $h \geqslant 0$, c — вещественное,

$$S = \sum_{x=0}^{m-1} \left\{ \frac{ax + \psi(x)}{m} \right\},$$

где $\psi(x)$ для рассматриваемых значений x принимает значения с условием $c \leqslant \psi(x) \leqslant c + h$. Доказать, что

$$\left| S - \frac{1}{2} m \right| \leqslant h + \frac{1}{2}.$$

b. Пусть M — целое, $m > 0$, $(a, m) = 1$, A и B — вещественные,

$$A = \frac{a}{m} + \frac{\lambda}{m^2}; \quad S = \sum_{x=M}^{M+m-1} \{Ax + B\}.$$

Доказать, что

$$\left| S - \frac{1}{2} m \right| \leqslant |\lambda| + \frac{1}{2}.$$

c. Пусть M — целое, $m > 0$, $(a, m) = 1$,

$$S = \sum_{x=M}^{M+m-1} \{f(x)\}.$$

где в интервале $M \leqslant x \leqslant M+m-1$ функция $f(x)$ имеет непрерывные производные $f'(x)$ и $f''(x)$, причём выполняются условия

$$f'(M)=\frac{a}{m}+\frac{\theta}{m^2};\ (a,m)=1;\ |\theta|<1,\ \frac{1}{A}\leqslant|f''(x)|\leqslant\frac{k}{A},$$

где

$$1\leqslant m\leqslant\tau,\ \tau=A^{\frac{1}{3}},\ A\geqslant 2,\ k\geqslant 1.$$

Доказать, что

$$\left|S-\frac{1}{2}m\right|<\frac{k+3}{2}.$$

4. Пусть в разложении иррационального числа A в непрерывную дробь все неполные частные ограничены, M — целое, m — целое, $m>0$, B — вещественное. Доказать, что

$$\sum_{x=M}^{M+m-1}(Ax+B)=\frac{1}{2}m+O(\ln m).$$

5, a. Пусть $A>2$, $k\geqslant 1$ и в интервале $Q\leqslant x\leqslant R$ функция $f(x)$ имеет вторую непрерывную производную, удовлетворяющую условиям

$$\frac{1}{A}\leqslant|f''(x)|\leqslant\frac{k}{A}.$$

Доказать, что

$$\sum_{Q<x\leqslant R}(f(x))=\frac{1}{2}(R-Q)+\theta\lambda;\ |\theta|<1$$

$$\lambda=(2k^2(R-Q)\ln A+8kA)A^{-\frac{1}{3}}.$$

b. Пусть $0<\sigma\leqslant 1$, Q и R — целые. При условиях вопроса a доказать, что число $\psi(\sigma)$ дробей $(f(x))$; $x=Q+1,\ldots,R$ с условием $0\leqslant(f(x))<\sigma$ выражается формулой

$$\psi(\sigma)=\sigma(R-Q)+\theta'\cdot 2\lambda;\ |\theta'|<1.$$

6, a. Пусть T — число целых точек (x, y) области $x^2+y^2\leqslant r^2$ $(r\geqslant 2)$. Доказать, что

$$T=\pi r^2+O(r^{\frac{2}{3}}\ln r).$$

b. Пусть n — целое, $n>2$, E — постоянная Эйлера. Доказать, что

$$\tau(1)+\tau(2)+\ldots+\tau(n)=n(\ln n+2E-1)+O\left(n^{\frac{1}{3}}(\ln n)^3\right).$$

7. Систему n целых положительных чисел, каждое из которых представлено в системе исчисления с основанием 2, назовём правильной, если при всяком целом неотрицательном s число чисел, в представление которых входит 2^s, будет чётным, и неправильной, если хотя бы при одном s это число будет нечётным.

Доказать, что неправильную систему путём уменьшения или полного изъятия некоторого одного её члена можно сделать правильной, а правильная система от уменьшения или полного изъятия любого её члена делается неправильной.

8, a. Доказать, что форма

$$3^n x_n+3^{n-1}x_{n-1}+\ldots+3x_1+x_0,$$

где $x_n, x_{n-1}, \ldots, x_1, x_0$ независимо друг от друга пробегают значения $-1, 0, 1$, представляет все числа

$$-H, \ldots, -1, 0, 1, \ldots, H;\ H=\frac{3^{n+1}-1}{3-1},$$

причём каждое число — единственным способом.

b. Пусть $m_1, m_2, \ldots, m_k$ — положительные попарно простые. Пользуясь c, § 4, доказать, что полную систему вычетов по модулю $m_1m_2\ldots m_k$ получим, заставляя в форме

$$x_1+m_1x_2+m_1m_2x_3+\ldots+m_1m_2\ldots m_{k-1}x_k$$

числа $x_1, x_2, \ldots, x_k$ пробегать полные системы вычетов по модулям $m_1, m_2, \ldots, m_k$.

9. Пусть $m_1, m_2, \ldots, m_k$ — попарно простые и

$$m_1m_2\ldots m_k=M_1m_1=M_2m_2=\ldots=M_km_k.$$

a. Применяя c, § 4, доказать, что полную систему вычетов по модулю $m_1m_2\ldots m_k$ получим, заставляя в форме

$$M_1x_1+M_2x_2+\ldots+M_kx_k$$

числа $x_1, x_2, \ldots, x_k$ пробегать полные системы вычетов по модулям $m_1, m_2, \ldots, m_k$.

b. Применяя c, § 4, гл. II и b, § 5, доказать, что приведённую систему вычетов по модулю $m_1m_2\ldots m_k$ получим, заставляя в форме

$$M_1x_1+M_2x_2+\ldots+M_kx_k$$

числа $x_1, x_2, \ldots, x_k$ пробегать приведённые системы вычетов по модулям $m_1, m_2, \ldots, m_k$.

c. Доказательство теоремы вопроса **b** провести независимо от теоремы c, § 4, гл. II и тогда уже вывести последнюю теорему, как следствие первой.

d. Найти элементарным путём выражение для $\varphi(p^\alpha)$ и, пользуясь равенством e, § 4 гл. II, вывести известное выражение для $\varphi(a)$.

10. Пусть $m_1, m_2, \ldots, m_k$ — попарно простые, превосходящие 1, $m = m_1 m_2 \ldots m_k$, $m = M_s m_s$.

a. Пусть $x_1, x_2, \ldots, x_k, x$ пробегают полные, а $\xi_1, \xi_2, \ldots, \xi_k, \xi$ — приведённые системы вычетов по модулям $m_1, m_2, \ldots, m_k, m$. Доказать, что дроби

$$\left\{\frac{x_1}{m_1}+\frac{x_2}{m_2}+\ldots+\frac{x_k}{m_k}\right\}$$

совпадают с дробями $\left\{\frac{x}{m}\right\}$, а дроби $\left\{\frac{\xi_1}{m_1}+\frac{\xi_2}{m_2}+\ldots+\frac{\xi_k}{m_k}\right\}$ совпадают с дробями $\left\{\frac{\xi}{m}\right\}$.

b. Пусть заданы k целых рациональных функций с целыми коэффициентами от r переменных $x, \ldots, w$ $(r \geqslant 1)$:

$$f_s(x, \ldots, w) = \sum_{\alpha, \ldots, \delta} c^{(s)}_{\alpha, \ldots, \delta} x^\alpha \ldots w^\delta; \quad s = 1, \ldots, k,$$

и пусть

$$f(x, \ldots, w) = \sum_{\alpha, \ldots, \delta} c_{\alpha, \ldots, \delta} x^\alpha \ldots w^\delta; \quad c_{\alpha, \ldots, \delta} = \sum_{s=1}^{k} M_s c^{(s)}_{\alpha, \ldots, \delta};$$

$x_s, \ldots, w_s$ пробегают полные, а $\xi_s, \ldots, \omega_s$ — приведённые системы вычетов по модулю m_s; $x, \ldots, w$ пробегают полные, а $\xi, \ldots, \omega$ — приведённые системы вычетов по модулю m. Доказать, что дроби $\left\{\frac{f_1(x_1, \ldots, w_1)}{m_1}+\ldots+\frac{f_k(x_k, \ldots, w_k)}{m_k}\right\}$ совпадают с дробями $\left\{\frac{f(x, \ldots, w)}{m}\right\}$, а дроби $\left\{\frac{f_1(\xi_1, \ldots, \omega_1)}{m_1}+\ldots+\frac{f_k(\xi_k, \ldots, \omega_k)}{m_k}\right\}$ совпадают с дробями $\left\{\frac{f(\xi, \ldots, \omega)}{m}\right\}$ (обобщение теорем вопроса a).

11, a. Пусть m — целое, $m > 0$, a — целое, x пробегает полную систему вычетов по модулю m. Доказать, что

$$\sum e^{2\pi i \frac{ax}{m}} = \begin{cases} m, & \text{если } a \text{ кратно } m, \\ 0 & \text{в противном случае.} \end{cases}$$

b. Пусть α — вещественное, M — целое, P — целое, $P > 0$. Обозначая символом (α) численное значение разности между α и ближайшим к α целым числом (расстояние α до ближайшего целого), доказать, что

$$\left|\sum_{x=M}^{M+P-1} e^{2\pi i \alpha x}\right| < \min\left(P, \frac{1}{h(\alpha)}\right); \quad h \geqslant \begin{cases} 2 \text{ всегда} \\ 3, \text{ при } (\alpha) \leqslant \frac{1}{6}. \end{cases}$$

c. Пусть m — целое, $m > 1$ и функции $M(a)$ и $P(a)$ для значений $a = 1, 2, \ldots, m-1$ принимают целые значения с условием $P(a) > 0$. Доказать, что

$$\sum_{a=1}^{m-1} \left|\sum_{x=M(a)}^{M(a)+P(a)-1} e^{2\pi i \frac{a}{m} x}\right| < \begin{cases} m \ln m - \frac{m}{3} \ln\left(2\left[\frac{m}{6}\right]+1\right), \\ m \ln m - \frac{m}{2}, \text{ при } m \geqslant 12, \\ m \ln m - m, \text{ при } m \geqslant 60. \end{cases}$$

12, a. Пусть m — целое, $m > 0$, ξ пробегает приведённую систему вычетов по модулю m. Доказать, что

$$\mu(m) = \sum_{\xi} e^{2\pi i \frac{\xi}{m}}.$$

b. Пользуясь теоремой вопроса a, доказать первую из теорем c, § 3, гл. II (см. решение вопроса 28, a, гл. II).

c. Теорему вопроса a вывести, пользуясь теоремой вопроса 17, a, гл. II.

d. Пусть

$$f(x, \ldots, w) = \sum_{\alpha, \ldots, \delta} c_{\alpha, \ldots, \delta} x^\alpha \ldots w^\delta$$

— целая рациональная функция с целыми коэффициентами от r переменных $x, \ldots, w$ $(r \geqslant 1)$, a — целое, m — целое, $m > 0$; $x, \ldots, w$ пробегают полные, а $\xi, \ldots, \omega$ — приведённые системы вычетов по модулю m. Вводим обозначения

$$S_{a,m} = \sum_{x} \cdots \sum_{w} e^{2\pi i \frac{af(x, \ldots, w)}{m}}, \quad S'_{a,m} = \sum_{\xi} \cdots \sum_{\omega} e^{2\pi i \frac{af(\xi, \ldots, \omega)}{m}}.$$

Пусть далее $m = m_1 \ldots m_k$, где $m_1, \ldots, m_k$ — попарно простые, превосходящие 1, и пусть $m = M_s m_s$. Доказать, что

$$S_{a_1, m_1} \ldots S_{a_k, m_k} = S_{M_1 a_1 + \ldots + M_k a_k, m},$$

$$S'_{a_1, m_1} \ldots S'_{a_k, m_k} = S'_{M_1 a_1 + \ldots + M_k a_k, m}.$$

c. При обозначениях вопроса d полагаем

$$A(m)=m^{-r}\sum_{a} S_{a,m},\quad A'(m)=m^{-r}\sum_{a} S'_{a,m},$$

где a пробегает приведённую систему вычетов по модулю m.
Доказать, что

$$A(m_1)\dots A(m_k)=A(m),\quad A'(m_1)\dots A'(m_k)=A'(m).$$

13, a. Доказать, что

$$\varphi(a)=\sum_{n=0}^{a-1}\prod_{p}\left(1-\frac{1}{p}\sum_{x=0}^{p-1}e^{2\pi i\frac{nx}{p}}\right),$$

где p пробегает простые делители числа a.
b. Из тождества вопроса **a** вывести известное выражение для $\varphi(a)$.
14. Доказать, что

$$\tau(a)=\lim_{\varepsilon\to 0}2\varepsilon\sum_{0<x<\sqrt{a}}\sum_{k=1}^{\infty}\frac{e^{2\pi i\frac{ak}{x}}}{k^{1+\varepsilon}}+\delta,$$

где $\delta=1$ или $\delta=0$, в зависимости от того, является ли a квадратом целого числа или нет.
15, a. Пусть p — простое и $h_1, h_2, \dots, h_n$ — целые. Доказать, что

$$(h_1+h_2+\dots+h_n)^p\equiv h_1^p+h_2^p+\dots+h_n^p \pmod p.$$

b. Из теоремы вопроса **a** вывести теорему Ферма.
c. Из теоремы Ферма вывести теорему Эйлера.

Численные примеры к главе III.

1, a. Найти остаток от деления

$$(12\,371^{56}+34)^{28} \text{ на } 111.$$

b. Делится ли на $1\,093^2$ число $2^{1092}-2$?
2, a. Применяя признаки делимости вопроса 1, найти каноническое разложение числа 244 943 325.
b. Найти каноническое разложение числа 282 321 246 671 737.

ГЛАВА ЧЕТВЁРТАЯ.

СРАВНЕНИЯ С ОДНИМ НЕИЗВЕСТНЫМ.

§ 1. Основные понятия.

Нашей ближайшей задачей будет изучение сравнений такого общего вида:

$$f(x)\equiv 0 \pmod m;\quad f(x)=ax^n+a_1x^{n-1}+\dots+a_n. \qquad (1)$$

Если a не делится на m, то n называется *степенью сравнения*.

Решить сравнение — значит найти все значения x, ему удовлетворяющие. Два сравнения, которым удовлетворяют одни и те же значения x, называются *равносильными*.

Если сравнению (1) удовлетворяет какое-либо $x=x_1$, то (d, § 2, гл. III) тому же сравнению будут удовлетворять и все числа, сравнимые с x_1 по модулю m: $x\equiv x_1 \pmod m$. Весь этот класс чисел считается за *одно решение*. При таком соглашении *сравнение (1) будет иметь столько решений, сколько вычетов полной системы ему удовлетворяет*.

Пример. Сравнению

$$x^5+x+1\equiv 0 \pmod 7$$

среди чисел: 0, 1, 2, 3, 4, 5, 6 полной системы вычетов по модулю 7 удовлетворяют два числа: $x=2$ и $x=4$. Поэтому указанное сравнение имеет два решения:

$$x\equiv 2 \pmod 7,\quad x\equiv 4 \pmod 7.$$

§ 2. Сравнения первой степени.

a. Сравнение первой степени перенесением свободного члена (с обратным знаком) в правую часть можно привести к виду

$$ax \equiv b \pmod{m}. \tag{1}$$

b. Приступая к исследованию вопроса о числе решений, мы сначала ограничим сравнение условием $(a, m) = 1$. Согласно § 1 наше сравнение имеет столько решений, сколько вычетов полной системы ему удовлетворяет. Но когда x пробегает полную систему вычетов по модулю m, то ax пробегает полную систему вычетов (d, § 4, гл. III). Следовательно, в частности, при одном и только одном значении x, взятом из полной системы, ax будет сравнимо с b. Итак, при $(a, m) = 1$ сравнение (1) имеет одно решение.

c. Пусть теперь $(a, m) = d > 1$. Тогда, чтобы сравнение (1) имело решения, необходимо (e, § 3, гл. III), чтобы b делилось на d, иначе сравнение (1) невозможно ни при каком целом x. Предполагая поэтому b кратным d, положим $a = a_1 d$, $b = b_1 d$, $m = m_1 d$. Тогда сравнение (1) будет равносильно такому (по сокращении на d): $a_1 x \equiv b_1 \pmod{m_1}$, в котором уже $(a_1, m_1) = 1$, и потому оно будет иметь одно решение по модулю m_1. Пусть x_1 — наименьший неотрицательный вычет этого решения по модулю m_1, тогда все числа x, образующие это решение, найдутся в форме

$$x \equiv x_1 \pmod{m_1}. \tag{2}$$

По модулю же m числа (2) образуют не одно решение, а больше, именно столько решений, сколько чисел (2) найдётся в ряде $0, 1, 2, \ldots, m-1$ наименьших неотрицательных вычетов по модулю m. Но сюда попадут следующие числа (2):

$$x_1,\ x_1 + m_1,\ x_1 + 2m_1,\ \ldots,\ x_1 + (d-1)m_1,$$

т. е. всего d чисел (2), следовательно, сравнение (1) имеет d решений.

d. Собирая всё доказанное, получаем теорему:

Пусть $(a, m) = d$. *Сравнение* $ax \equiv b \pmod{m}$ *невозможно, если* b *не делится на* d. *При* b, *кратном* d, *сравнение имеет* d *решений.*

e. Обращаясь к разысканию решений сравнения (1), мы укажем только способ, основанный на теории непрерывных дробей, причём достаточно ограничиться лишь случаем $(a, m) = 1$.

Разлагая в непрерывную дробь отношение $m : a$,

$$\frac{m}{a} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \cfrac{1}{q_n}}}}$$

и рассматривая две последние подходящие дроби:

$$\frac{P_{n-1}}{Q_{n-1}},\ \frac{P_n}{Q_n} = \frac{m}{a},$$

согласно свойствам непрерывных дробей (e, § 4, гл. I) имеем

$$mQ_{n-1} - aP_{n-1} = (-1)^n,$$
$$aP_{n-1} \equiv (-1)^{n-1} \pmod{m},$$
$$a \cdot (-1)^{n-1} P_{n-1} b \equiv b \pmod{m}.$$

Итак, наше сравнение имеет решение

$$x \equiv (-1)^{n-1} P_{n-1} b \pmod{m},$$

для разыскания которого достаточно вычислить P_{n-1} согласно способу, указанному в d, § 4, гл. I.

Пример. Решим сравнение

$$111x \equiv 75 \pmod{321}. \tag{3}$$

Здесь $(111, 321) = 3$, причём 75 кратно 3. Поэтому сравнение имеет три решения.

Деля обе части сравнения и модуль на 3, получим сравнение

$$37x \equiv 25 \pmod{107}. \tag{4}$$

которое нам следует сначала решить. Имеем

$$\begin{array}{r|l} 107 & 37 \\ 74 & 2 \\ \hline 37 & 33 \\ 33 & 1 \\ \hline 33 & 4 \\ 32 & 8 \\ \hline 4 & 1 \\ 4 & 4 \\ \hline 0 & \end{array}$$

q		2	1	8	4
P_s	1	2	3	26	107

Значит, в данном случае $n=4$, $P_{n-1}=26$, $b=25$, и мы имеем решение сравнения (4) в форме

$$x \equiv -26 \cdot 25 \equiv 99 \pmod{107}.$$

Отсюда решения сравнения (3) представляются так:

$$x \equiv 99;\ 99+107;\ 99+2\cdot 107 \pmod{321},$$

т. е.

$$x \equiv 99;\ 206;\ 313 \pmod{321}.$$

§ 3. Система сравнений первой степени.

a. Мы рассмотрим лишь простейшую систему сравнений

$$x \equiv b_1 \pmod{m_1},\quad x \equiv b_2 \pmod{m_2},\ \ldots,\ x \equiv b_k \pmod{m_k} \quad (1)$$

с одним неизвестным, но с разными и притом попарно простыми модулями.

b. Решить систему (1), т. е. найти все значения x, ей удовлетворяющие, можно применяя следующую теорему:

Пусть числа M_s и M'_s определены из условий

$$m_1 m_2 \ldots m_k = M_s m_s,\quad M_s M'_s \equiv 1 \pmod{m_s}$$

и пусть

$$x_0 = M_1 M'_1 b_1 + M_2 M'_2 b_2 + \ldots + M_k M'_k b_k$$

Тогда совокупность значений x, удовлетворяющих системе (1), определяется сравнением

$$x \equiv x_0 \pmod{m_1 m_2 \ldots m_k}. \quad (2)$$

Действительно, ввиду делимости на m_s всех M_p, отличных от M_s, при любом $s=1, 2, \ldots, k$ имеем

$$x_0 \equiv M_s M'_s b_s \equiv b_s \pmod{m_s},$$

и, таким образом, системе (1) удовлетворяет $x=x_0$. Отсюда непосредственно следует, что система (1) равносильна системе

$$x \equiv x_0 \pmod{m_1},\ x \equiv x_0 \pmod{m_2},\ \ldots,\ x \equiv x_0 \pmod{m_k} \quad (3)$$

(т. е. что системам (1) и (3) удовлетворяют одни и те же значения x). Системе же (3), ввиду теорем c, § 3, гл. III и d, § 3, гл. III, удовлетворяют те и только те значения x, которые удовлетворяют сравнению (2).

c. *Если $b_1, b_2, \ldots, b_k$ независимо друг от друга пробегают полные системы вычетов по модулям $m_1, m_2, \ldots, m_k$, то x_0 пробегает полную систему вычетов по модулю $m_1 m_2 \ldots m_k$.*

Действительно, x_0 пробегает $m_1 m_2 \ldots m_k$ значений, ввиду d, § 3, гл. III, несравнимых по модулю $m_1 m_2 \ldots m_k$.

d. Пример. Решим систему

$$x \equiv b_1 \pmod 4,\quad x \equiv b_2 \pmod 5,\quad x \equiv b_3 \pmod 7.$$

Здесь $4 \cdot 5 \cdot 7 = 35 \cdot 4 = 28 \cdot 5 = 20 \cdot 7$, причём

$$35 \cdot 3 \equiv 1 \pmod 4,\quad 28 \cdot 2 \equiv 1 \pmod 5,\quad 20 \cdot 6 \equiv 1 \pmod 7.$$

Поэтому

$$x_0 = 35 \cdot 3b_1 + 28 \cdot 2b_2 + 20 \cdot 6b_3 = 105b_1 + 56b_2 + 120b_3$$

и, следовательно, совокупность значений x, удовлетворяющих системе, может быть представлена в форме

$$x \equiv 105b_1 + 56b_2 + 120b_3 \pmod{140}.$$

Так, например, совокупность значений x, удовлетворяющих системе

$$x \equiv 1 \pmod 4, \quad x \equiv 3 \pmod 5, \quad x \equiv 2 \pmod 7,$$

будет

$$x \equiv 105 \cdot 1 + 56 \cdot 3 + 120 \cdot 2 \equiv 93 \pmod{140},$$

а совокупность значений x, удовлетворяющих системе

$$x \equiv 3 \pmod 4, \quad x \equiv 2 \pmod 5, \quad x \equiv 6 \pmod 7,$$

будет

$$x = 105 \cdot 3 + 56 \cdot 2 + 120 \cdot 6 \equiv 27 \pmod{140}.$$

§ 4. Сравнения любой степени по простому модулю.

a. Пусть p — простое. Докажем общие теоремы, относящиеся к сравнению вида

$$f(x) \equiv 0 \pmod p; \quad f(x) = ax^n + a_1x^{n-1} + \ldots + a_n. \quad (1)$$

b. *Сравнение вида* (1) *равносильно сравнению степени не выше* $p-1$.

Действительно, деля $f(x)$ на $x^p - x$, имеем

$$f(x) = (x^p - x)\,Q(x) + R(x),$$

где степень $R(x)$ не выше $p-1$. А так как $x^p - x \equiv 0 \pmod p$, то $f(x) \equiv R(x) \pmod p$, откуда и следует указанная теорема.

c. *Если сравнение* (1) *имеет более чем* n *решений, то все коэффициенты* $f(x)$ *кратны* p.

Действительно, пусть сравнение (1) имеет, по крайней мере, $n+1$ решение. Обозначая буквами $x_1, x_2, \ldots, x_n, x_{n+1}$ вычеты этих решений, мы можем $f(x)$ представить в форме

$$\begin{aligned} f(x) = {} & a(x-x_1)(x-x_2)\ldots(x-x_{n-2})(x-x_{n-1})(x-x_n) + \\ & + b(x-x_1)(x-x_2)\ldots(x-x_{n-2})(x-x_{n-1}) + \\ & + c(x-x_1)(x-x_2)\ldots(x-x_{n-2}) + \\ & + \ldots\ldots\ldots\ldots\ldots\ldots + \\ & + k(x-x_1)(x-x_2) + \\ & + l(x-x_1) + \\ & + m. \end{aligned} \quad (2)$$

Для этой цели, преобразовав (раскрытием скобок) слагаемые правой части в многочлены, выберем b так, чтобы сумма коэффициентов при x^{n-1} двух первых многочленов совпала с a_1; зная b, выберем c так, чтобы сумма коэффициентов при x^{n-2} трёх первых многочленов совпала с a_2, и т. д.

Полагая в (2) последовательно $x = x_1, x_2, \ldots, x_n, x_{n+1}$, убеждаемся в том, что все $m, l, k, \ldots, c, b, a$ кратны p. Значит, и все $a, a_1, \ldots, a_n$ кратны p (как суммы чисел, кратных p).

d. *При простом* p *справедливо сравнение (теорема Вильсона)*

$$1 \cdot 2 \ldots (p-1) + 1 \equiv 0 \pmod p. \quad (3)$$

Действительно, если $p = 2$, то теорема очевидна. Если же $p > 2$, то рассмотрим сравнение

$$(x-1)(x-2)\ldots(x-(p-1)) - (x^{p-1}-1) \equiv 0 \pmod p;$$

оно степени не выше $p-2$ и имеет $p-1$ решение, именно решения с вычетами $1, 2, \ldots, p-1$. Следовательно, по теореме с все его коэффициенты кратны p; в частности, на p делится и свободный член, равный как раз левой части сравнения (3).

Пример. Имеем $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 + 1 = 721 \equiv 0 \pmod 7$.

§ 5. Сравнения любой степени по составному модулю.

a. *Если* $m_1, m_2, \ldots, m_k$ *попарно простые, то сравнение*

$$f(x) \equiv 0 \pmod{m_1 m_2 \ldots m_k} \quad (1)$$

равносильно системе

$$f(x) \equiv 0 \pmod{m_1},$$
$$f(x) \equiv 0 \pmod{m_2}, \ \ldots, \ f(x) \equiv 0 \pmod{m_k}.$$

При этом, обозначая через $T_1, T_2, \ldots, T_k$ *числа решений отдельных сравнений этой системы по соответственным модулям и через* T *— число решений сравнения* (1), *будем иметь*

$$T = T_1 T_2 \ldots T_k.$$

Действительно, первая часть теоремы следует из c и d, § 3, гл III. Вторая часть следует из того, что каждое сравнение

$$f(x) \equiv 0 \pmod{m_s} \qquad (2)$$

выполняется тогда и только тогда, когда выполняется одно из T_s сравнений вида

$$x \equiv b_s \pmod{m_s},$$

где b_s пробегает вычеты решений сравнения (2), причём возможно всего $T_1 T_2 \ldots T_k$ различных комбинаций вида

$$x \equiv b_1 \pmod{m_1},\ x \equiv b_2 \pmod{m_2},\ \ldots,\ x \equiv b_k \pmod{m_k},$$

приводящих (c, § 3) к различным классам по модулю

$$m_1 m_2 \ldots m_k.$$

Пример. Сравнение

$$f(x) \equiv 0 \pmod{35},\quad f(x) = x^4 + 2x^3 + 8x + 9 \qquad (3)$$

равносильно системе

$$f(x) \equiv 0 \pmod{5},\ f(x) \equiv 0 \pmod{7}.$$

Легко убедимся (§ 1), что первое сравнение этой системы имеет 2 решения: $x \equiv 1;\ 4 \pmod 5$, второе же сравнение имеет 3 решения: $x \equiv 3;\ 5;\ 6 \pmod 7$. Поэтому сравнение (3) имеет $2 \cdot 3 = 6$ решений. Чтобы найти эти 6 решений, надо решить 6 систем вида

$$x \equiv b_1 \pmod 5,\quad x \equiv b_2 \pmod 7, \qquad (4)$$

которые получим, заставляя b_1 пробегать значения $b_1 = 1;\ 4$, а b_2 пробегать значения $b_2 = 3;\ 5;\ 6$. Но, ввиду

$$35 = 7 \cdot 5 = 5 \cdot 7,\quad 7 \cdot 3 \equiv 1 \pmod 5,\quad 5 \cdot 3 \equiv 1 \pmod 7,$$

совокупность значений x, удовлетворяющих системе (4), представится в форме (b, § 3)

$$x \equiv 21\, b_1 + 15\, b_2 \pmod{35}.$$

Поэтому решения сравнения (3) будут

$$x \equiv 31;\ 26;\ 6;\ 24;\ 19;\ 34 \pmod{35}.$$

b. Ввиду теоремы a исследование и решение сравнения

$$f(x) \equiv 0 \pmod{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}}$$

сводятся к исследованию и решению сравнений вида

$$f(x) \equiv 0 \pmod{p^\alpha}; \qquad (5)$$

это же последнее сравнение сводится вообще, как мы сейчас выясним, к сравнению

$$f(x) \equiv 0 \pmod p. \qquad (6)$$

Действительно, всякое x, удовлетворяющее сравнению (5), необходимо должно удовлетворять и сравнению (6). Пусть

$$x \equiv x_1 \pmod p$$

—какое-либо решение сравнения (6). Тогда $x = x_1 + pt_1$, где t_1 — целое. Вставляя это значение x в сравнение

$$f(x) \equiv 0 \pmod{p^2}$$

и разлагая левую часть по формуле Тейлора, найдём (принимая во внимание, что $\frac{1}{k!} f^{(k)}(x_1)$ — целое, и отбрасывая члены, кратные p^2)

$$f(x_1) + pt_1 f'(x_1) \equiv 0 \pmod{p^2},\quad \frac{f(x_1)}{p} + t_1 f'(x_1) \equiv 0 \pmod p.$$

Ограничиваясь здесь случаем, когда $f'(x_1)$ не делится на p, имеем одно решение:

$$t_1 \equiv t_1' \pmod p;\quad t_1 = t_1' + pt_2.$$

Выражение для x принимает вид

$$x = x_1 + pt_1' + p^2 t_2 = x_2 + p^2 t_2;$$

вставляя его в сравнение

$$f(x) \equiv 0 \pmod{p^3},$$

получим

$$f(x_2) + p^2 t_2 f'(x_2) \equiv 0 \pmod{p^3},$$

$$\frac{f(x_2)}{p^2} + t_2 f'(x_2) \equiv 0 \pmod{p}.$$

Здесь $f'(x_2)$ не делится на p, так как

$$x_2 \equiv x_1 \pmod{p},$$

$$f'(x_2) \equiv f'(x_1) \pmod{p},$$

и потому последнее сравнение имеет одно решение:

$$t_2 \equiv t_2' \pmod{p};$$

$$t_2 = t_2' + pt_3.$$

Выражение для x принимает вид

$$x = x_2 + p^2 t_2' + p^3 t_3 = x_3 + p^3 t_3;$$

и т. д. Таким путём по данному решению сравнения (6) постепенно найдём сравнимое с ним решение сравнения (5). Итак, *всякое решение* $x \equiv x_1 \pmod{p}$ *сравнения* (6) *при условии, что* $f'(x_1)$ *не делится на* p, *даст одно решение сравнения* (5):

$$x = x_\alpha + p^\alpha t_\alpha;$$

$$x \equiv x_\alpha \pmod{p^\alpha}.$$

Пример. Решим сравнение

$$\left.\begin{aligned} f'(x) &\equiv 0 \pmod{27}; \\ f(x) &= x^4 + 7x + 4. \end{aligned}\right\} \qquad (7)$$

Сравнение $f(x) \equiv 0 \pmod 3$ имеет одно решение $x \equiv 1 \pmod 3$; при этом $f'(1) \equiv 2 \pmod 3$ и, следовательно, не делится на 3. Находим:

$$x = 1 + 3t_1,$$

$$f(1) + 3t_1 f'(1) \equiv 0 \pmod 9, \quad 3 + 3t_1 \cdot 2 \equiv 0 \pmod 9,$$

$$2t_1 + 1 \equiv 0 \pmod 3, \quad t_1 \equiv 1 \pmod 3, \quad t_1 = 1 + 3t_2,$$

$$x = 4 + 9t_2,$$

$$f(4) + 9t_2 f'(4) \equiv 0 \pmod{27}, \quad 18 + 9t_2 \cdot 2 \equiv 0 \pmod{27},$$

$$2t_2 + 2 \equiv 0 \pmod 3, \quad t_2 \equiv 2 \pmod 3, \quad t_2 = 2 + 3t_3,$$

$$x = 22 + 27t_3.$$

Таким образом сравнение (7) имеет одно решение:

$$x \equiv 22 \pmod{27}.$$

Вопросы к главе IV.

1, a. Пусть m — целое, $m > 0$, $f(x, \ldots, w)$ — целая рациональная функция с целыми коэффициентами от r переменных $x, \ldots, w$ ($r \geqslant 1$). Если сравнению

$$f(x, \ldots, w) \equiv 0 \pmod m \qquad (1)$$

удовлетворяет система $x = x_0, \ldots, w = w_0$, то (обобщение определения § 1) систему классов чисел по модулю m:

$$x \equiv x_0 \pmod m, \ \ldots, \ w \equiv w_0 \pmod m$$

будем считать за одно решение сравнения (1).

Пусть T — число решений сравнения (1). Доказать, что

$$Tm = \sum_{\alpha=0}^{m-1} \sum_{x=0}^{m-1} \cdots \sum_{w=0}^{m-1} e^{2\pi i \frac{\alpha f(x, \ldots, w)}{m}}.$$

b. При обозначениях вопроса **a** и вопроса **12, e**, гл. **III** доказать, что

$$Tm = m^r \sum_{m_0 \backslash m} A(m_0).$$

c. Равенство вопроса **a** применить к доказательству теоремы о числе решений сравнения первой степени.

d. Пусть m — целое, $m > 0$; $a, \ldots, f, g$ — целые, их число равно $r + 1$ ($r > 0$): $d = (a, \ldots, f, m)$; T — число решений сравнения

$$ax + \ldots + fw + g \equiv 0 \pmod m.$$

Пользуясь равенством вопроса **a**, доказать, что

$$T=\begin{cases} m^{r-1}d, & \text{если } g \text{ кратно } d, \\ 0 & \text{в противном случае.} \end{cases}$$

c. Теорему вопроса **d** доказать, исходя из теоремы о числе решений сравнения $ax \equiv b \pmod m$.

2, a. Пусть $m > 1$, $(a, m)=1$. Доказать, что сравнение $ax \equiv b \pmod m$ имеет решение $x \equiv ba^{\varphi(m)-1} \pmod m$.

b. Пусть p — простое, $0 < a < p$. Доказать, что сравнение $ax \equiv b \pmod p$ имеет решение

$$x \equiv b(-1)^{a-1}\frac{(p-1)(p-2)\dots(p-a+1)}{1\cdot 2\dots a} \pmod p.$$

c, α) Указать возможно более простой способ решения сравнения вида

$$2^k_0 x \equiv b \pmod m; \qquad (2, m)=1.$$

β) Указать возможно более простой способ решения сравнения вида

$$3^k x \equiv b \pmod m; \qquad (3, m)=1.$$

γ) Пусть $(a, m)=1$, $1 < a < m$. Развивая способы, указанные в вопросах α) и β), доказать, что разыскание решения сравнения $ax \equiv b \pmod m$ может быть приведено к разысканию решений сравнений вида $b + mt \equiv 0 \pmod p$, где p — простой делитель числа a.

3. Пусть m — целое, $m > 1$, $1 \leqslant \tau < m$, $(a, m)=1$. Пользуясь теорией сравнений, доказать существование целых x и y с условиями

$$ax \equiv y \pmod m, \quad 0 < x \leqslant \tau, \quad 0 < |y| < \frac{m}{\tau}.$$

4, a. При $(a, m)=1$ будем рассматривать символическую дробь $\frac{b}{a}$ по модулю m, обозначающую любой вычет решения сравнения $ax \equiv b \pmod m$. Доказать, что (сравнения берутся по модулю m):

α) При $a \equiv a_1$, $b \equiv b_1$ имеем $\frac{b}{a} \equiv \frac{b_1}{a_1}$.

β) Числитель b символической дроби $\frac{b}{a}$ можно заменить сравнимым b_0, кратным a. Тогда символическая дробь $\frac{b}{a}$ сравнима с целым числом, представляемым обычной дробью $\frac{b_0}{a}$.

γ) $\frac{b}{a} + \frac{d}{c} \equiv \frac{bc+ad}{ac}$.

δ) $\frac{b}{a} \cdot \frac{d}{c} \equiv \frac{bd}{ac}$.

b, α) Пусть p — простое, $p > 2$, a — целое, $0 < a < p-1$. Доказать, что

$$\binom{p-1}{a} \equiv (-1)^a \pmod p.$$

β) Пусть p простое, $p > 2$. Доказать, что

$$\frac{2^p-2}{p} \equiv 1-\frac{1}{2}+\frac{1}{3}-\dots-\frac{1}{p-1} \pmod p.$$

5, a. Пусть d — делитель числа a, не делящийся на простые, меньшие n, и $\varkappa$ — число различных простых делителей числа d. Доказать, что в ряде

$$1\cdot 2\dots n, \quad 2\cdot 3\dots(n+1), \quad \dots, \quad a(a+1)\dots(a+n-1) \qquad (1)$$

чисел, кратных d, будет $\frac{n^\varkappa a}{d}$.

b. Пусть $p_1, p_2, \dots, p_k$ — различные простые делители числа a, причём ни один из них не меньше чем n. Доказать, что число чисел ряда (1), взаимно простых с a, будет

$$a\left(1-\frac{n}{p_1}\right)\left(1-\frac{n}{p_2}\right)\dots\left(1-\frac{n}{p_k}\right).$$

6. Пусть $m_{1,2,\dots,k}$ — общее наименьшее кратное чисел $m_1, m_2, \dots, m_k$.

a. Пусть $d=(m_1, m_2)$. Доказать, что система

$$x \equiv b_1 \pmod{m_1}, \quad x \equiv b_2 \pmod{m_2}$$

разрешима тогда и только тогда, когда $b_2 - b_1$ кратно d, причём в случае разрешимости совокупность значений x, удовлетворяющих этой системе, определяется сравнением вида

$$x \equiv x_{1,2} \pmod{m_{1,2}}.$$

b. Доказать, что в случае разрешимости системы

$$x \equiv b_1 \pmod{m_1}, \quad x \equiv b_2 \pmod{m_2}, \quad \dots, \quad x \equiv b_k \pmod{m_k}$$

совокупность значений x, ей удовлетворяющих, определяется сравнением вида

$$x \equiv x_{1,2,\dots,k} \pmod{m_{1,2,\dots,k}}.$$

7. Пусть m — целое, $m > 1$, a и b — целые,

$$\left(\frac{a, b}{m}\right) = \sum_x e^{2\pi i \frac{ax+bx'}{m}},$$

где x пробегает приведённую систему вычетов по модулю m, причём $x' \equiv \frac{1}{x} \pmod m$ (в смысле вопроса 4, a). Доказать следующие свойства символа $\left(\frac{a, b}{m}\right)$:

α) $\left(\frac{a, b}{m}\right)$ вещественное.

β) $\left(\frac{a, b}{m}\right) = \left(\frac{b, a}{m}\right)$.

γ) При $(h, m)=1$ имеем $\left(\frac{a, bh}{m}\right) = \left(\frac{ah, b}{m}\right)$.

δ) При $m_1, m_2, \ldots, m_k$ попарно простых, полагая $m_1 m_2 \ldots m_k = m$, $m = M_s m_s$, имеем

$$\left(\frac{a_1, 1}{m_1}\right)\left(\frac{a_2, 1}{m_2}\right)\cdots\left(\frac{a_k, 1}{m_k}\right) = \left(\frac{M_1^2 a_1 + M_2^2 a_2 + \ldots + M_k^2 a_k, 1}{m}\right).$$

8. Пусть сравнение

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_n \equiv 0 \pmod p$$

имеет n решений

$$x \equiv x_1, x_2, \ldots, x_n \pmod p.$$

Доказать, что

$$a_1 \equiv -a_0 S_1 \pmod p,$$
$$a_2 \equiv a_0 S_2 \pmod p,$$
$$a_3 \equiv -a_0 S_3 \pmod p,$$
$$\ldots\ldots\ldots$$
$$a_n \equiv (-1)^n a_0 S_n \pmod p,$$

где S_1 есть сумма всех x_s; S_2 — сумма произведений по два, S_3 — сумма произведений по три и т. д.

9, a. Доказать теорему Вильсона, рассматривая пары x, x' чисел ряда $2, 3, \ldots, p-2$, удовлетворяющие условию $xx' \equiv 1 \pmod p$.

b. Пусть P — целое, $P > 1$, $1 \cdot 2 \ldots (P-1) + 1 \equiv 0 \pmod P$. Доказать, что P — простое.

10, a. Пусть $(a_0, m)=1$. Указать сравнение n-й степени $(n > 0)$ со старшим коэффициентом 1, равносильное сравнению

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_n \equiv 0 \pmod m.$$

b. Доказать, что необходимое и достаточное условие того, что сравнение $f(x) \equiv 0 \pmod p$; $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$; $n < p$ имеет n решений, есть делимость на p всех коэффициентов остатка от деления $x^p - x$ на $f(x)$.

c. Пусть n — делитель $p-1$; $n > 1$; $(A, p)=1$. Доказать, что необходимое и достаточное условие разрешимости сравнения $x^n \equiv A \pmod p$ есть $A^{\frac{p-1}{n}} \equiv 1 \pmod p$, причём в случае разрешимости указанное сравнение имеет n решений.

11. Пусть n — целое, $n > 0$, $(A, m)=1$, и известно одно решение $x \equiv x_0 \pmod m$ сравнения $x^n \equiv A \pmod m$. Доказать, что все решения этого сравнения представятся произведением x_0 на вычеты решений сравнения $y^n \equiv 1 \pmod m$.

Численные примеры к главе IV.

1, a. Решить сравнение $256x \equiv 179 \pmod{337}$.

b. Решить сравнение $1215x \equiv 560 \pmod{2755}$.

2, a. Сравнения примеров 1, a и 1, b решить по способу вопроса 2, c.

b. Сравнение $1296x \equiv 1105 \pmod{2413}$ решить по способу вопроса 2, c.

3. Найти все пары x, y, удовлетворяющие неопределённому уравнению $47x - 111y = 89$.

4, a. Указать общее решение для системы

$$x \equiv b_1 \pmod{13}, \quad x \equiv b_2 \pmod{17}.$$

Пользуясь этим общим решением, далее найти три числа которые при делении на 13 и 17 давали бы соответственно остатки 1 и 12, 6 и 8, 11 и 4.

b. Указать общее решение для системы

$$x \equiv b_1 \pmod{25}, \quad x \equiv b_2 \pmod{27}, \quad x \equiv b_3 \pmod{59}.$$

5, a. Решить систему сравнений (вопрос 6, a)

$$x \equiv 3 \pmod 8, \quad x \equiv 11 \pmod{20}, \quad x \equiv 1 \pmod{15}.$$

b. Решить систему сравнений

$$x \equiv 1 \pmod 3, \quad x \equiv 4 \pmod 5, \quad x \equiv 2 \pmod 7,$$
$$x \equiv 9 \pmod{11}, \quad x \equiv 3 \pmod{13}.$$

6. Решить систему сравнений

$$3x + 4y - 29 \equiv 0 \pmod{143}, \quad 2x - 9y + 84 \equiv 0 \pmod{143}.$$

7, a. Какому сравнению степени ниже 5 равносильно сравнение

$$3x^{14} + 4x^{13} + 3x^{12} + 2x^{11} + x^9 + 2x^8 + 4x^7 + x^6 + 3x^4 + x^3 + 4x^2 + 2x \equiv 0 \pmod 5?$$

b. Какому сравнению степени ниже 7 равносильно сравнение

$$2x^{17}+6x^{16}+x^{14}+5x^{12}+3x^{11}+2x^{10}+x^9+5x^3+ \\ +2x^7+3x^5+4x^4+6x^3+4x^2+x+4\equiv 0 \pmod 7?$$

8. Какому сравнению со старшим коэффициентом 1 равносильно сравнение (вопрос 10, a)

$$70x^6+78x^5+25x^4+68x^3+52x^2+4x+3\equiv 0 \pmod{101}?$$

9, a. Решить сравнение

$$f(x)\equiv 0 \pmod{27}, \quad f(x)=7x^4+19x+25,$$

найдя сначала помощью проб все решения сравнения

$$f(x)\equiv 0 \pmod 3.$$

b. Решить сравнение $9x^2+29x+62\equiv 0 \pmod{64}$.
10, a. Решить сравнение $x^3+2x+2\equiv 0 \pmod{125}$.
b. Решить сравнение $x^4+4x^3+2x^2+2x+12\equiv 0 \pmod{625}$.
11, a. Решить сравнение $6x^3+27x^2+17x+20\equiv 0 \pmod{30}$.
b. Решить сравнение $31x^4+57x^3+96x+191\equiv 0 \pmod{225}$.

ГЛАВА ПЯТАЯ

СРАВНЕНИЯ ВТОРОЙ СТЕПЕНИ.

§ 1. Общие теоремы.

a. Из сравнений степени $n>1$ в дальнейшем будут рассматриваться лишь простейшие, а именно — *двучленные сравнения*:

$$x^n\equiv a \pmod m; \quad (a,m)=1. \tag{1}$$

Если сравнение (1) имеет решения, то a называется *вычетом степени* n, в противном случае a называется *невычетом степени* n. В частности, при $n=2$ вычеты или невычеты называются *квадратичными*, при $n=3$ — *кубическими*, при $n=4$ — *биквадратичными*.

b. В этой главе мы подробно рассмотрим случай $n=2$ и в первую очередь рассмотрим двучленные сравнения второй степени по простому нечётному модулю p:

$$x^2\equiv a \pmod p; \quad (a,\ p)=1. \tag{2}$$

c. *Если a — квадратичный вычет по модулю p, то сравнение (2) имеет два решения.*

Действительно, если a — квадратичный вычет, то сравнение (2) имеет, по крайней мере, одно решение $x\equiv x_1 \pmod p$. Но тогда, ввиду $(-x_1)^2=x_1^2$, то же сравнение имеет и второе решение $x\equiv -x_1 \pmod p$. Это второе решение отлично от первого, так как из $x_1\equiv -x_1 \pmod p$ мы имели бы $2x_1\equiv 0 \pmod p$, что невозможно, ввиду $(2,\ p)=(x_1,\ p)=1$.

Указанными двумя решениями и исчерпываются все решения сравнения (2), так как последнее, будучи

сравнением второй степени, более двух решений иметь не может (c, § 4, гл. IV).

d. *Приведённая система вычетов по модулю p состоит из $\frac{p-1}{2}$ квадратичных вычетов, сравнимых с числами*

$$1^2,\ 2^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2, \tag{3}$$

и $\left(\frac{p-1}{2}\right)$ квадратичных невычетов.

Действительно, среди вычетов приведённой системы по модулю p квадратичными вычетами являются те и только те, которые сравнимы с квадратами чисел (приведённая система вычетов)

$$-\frac{p-1}{2},\ \ldots,\ -2,\ -1,\ 1,\ 2,\ \ldots,\ \frac{p-1}{2}, \tag{4}$$

т. е. с числами (3). При этом числа (3) по модулю p не сравнимы, так как из $k^2 \equiv l^2 \pmod p$, $0 < k < l \leqslant \frac{p-1}{2}$, следовало бы, что сравнению $x^2 \equiv l^2 \pmod p$, вопреки c, среди чисел (4) удовлетворяют четыре: $x = -l, -k, k, l$.

e. *Если a — квадратичный вычет по модулю p, то*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p; \tag{5}$$

если a — квадратичный невычет по модулю p, то

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p. \tag{6}$$

Действительно, по теореме Ферма,

$$a^{p-1} \equiv 1 \pmod p; \qquad (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod p.$$

Один и только один из сомножителей левой части последнего сравнения делится на p (оба сомножителя не могут одновременно делиться на p, в противном случае их разность 2 должна была бы делиться на p). Поэтому имеет место одно и только одно из сравнений (5) и (6).

Но всякий квадратичный вычет a удовлетворяет при некотором x сравнению

$$a \equiv x^2 \pmod p \tag{7}$$

и, следовательно, удовлетворяет также и сравнению (5), которое можно получить почленным возведением (7) в степень $\frac{p-1}{2}$. При этом квадратичными вычетами и исчерпываются все решения сравнения (5), так как, будучи сравнением степени $\frac{p-1}{2}$, оно не может иметь более чем $\frac{p-1}{2}$ решений.

Поэтому квадратичные невычеты удовлетворяют сравнению (6).

§ 2. Символ Лежандра.

a. Введём в рассмотрение *символ Лежандра* $\left(\frac{a}{p}\right)$ (читается символ a по отношению к p). Этот символ определяется для всех a, не делящихся на p; он равен 1, если a — квадратичный вычет, и -1, если a — квадратичный невычет. Число a называется числителем, p — знаменателем символа.

b. Ввиду e, § 1, очевидно, имеем

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p.$$

c. Здесь мы выведем главнейшие свойства символа Лежандра и в следующем параграфе — свойства обобщения этого символа — символа Якоби, которые позволят быстро вычислять этот символ, а следовательно, решать вопрос о возможности сравнения

$$x^2 \equiv a \pmod p.$$

d. *Если $a \equiv a_1 \pmod p$, то $\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$.*

Это свойство следует из того, что числа одного и того же класса будут одновременно квадратичными вычетами или невычетами.

e. $\left(\frac{1}{p}\right)=1$.

Действительно, $1=1^2$ и, следовательно, 1 – квадратичный вычет.

f. $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

Это свойство следует из b при $a=-1$.

Так как $\frac{p-1}{2}$ чётное, если p формы $4m+1$, и нечётное, если p формы $4m+3$, то отсюда следует, что -1 является квадратичным вычетом простых чисел формы $4m+1$ и квадратичным невычетом простых чисел формы $4m+3$.

g. $\left(\frac{ab\dots l}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\dots\left(\frac{l}{p}\right)$.

Действительно, имеем

$$\left(\frac{ab\dots l}{p}\right)\equiv(ab\dots l)^{\frac{p-1}{2}}\equiv a^{\frac{p-1}{2}}b^{\frac{p-1}{2}}\dots l^{\frac{p-1}{2}}\equiv$$
$$\equiv\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\dots\left(\frac{l}{p}\right)\pmod p,$$

откуда и вытекает наше утверждение. Отсюда следствие:

$$\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right),$$

т. е. в числителе символа можно отбросить любой квадратичный множитель.

h. Для вывода дальнейших свойств символа Лежандра мы сначала дадим ему другое истолкование. Полагая $p_1=\frac{p-1}{2}$, рассмотрим сравнения

$$\left.\begin{aligned} a\cdot 1&\equiv\varepsilon_1 r_1\pmod p,\\ a\cdot 2&\equiv\varepsilon_2 r_2\pmod p,\\ &\dots\dots\dots\dots\\ a\cdot p_1&\equiv\varepsilon_{p_1} r_{p_1}\pmod p,\end{aligned}\right\}\qquad(1)$$

где $\varepsilon_x r_x$ – абсолютно наименьший вычет ax, r_x – его модуль, так что $\varepsilon_x=\pm 1$.

Числа $a\cdot 1$, $-a\cdot 1$, $a\cdot 2$, $-a\cdot 2$, …, $a\cdot p_1$, $-a\cdot p_1$ образуют приведённую систему вычетов по модулю p (c, § 5, гл. III); их абсолютно наименьшие вычеты суть $\varepsilon_1 r_1$, $-\varepsilon_1 r_1$, $\varepsilon_2 r_2$, $-\varepsilon_2 r_2$, …, $\varepsilon_{p_1} r_{p_1}$, $-\varepsilon_{p_1} r_{p_1}$. Положительные из последних, т. е. r_1, r_2, …, r_{p_1}, должны совпадать с числами 1, 2, …, p_1 (b, § 4, гл. III).

Перемножая теперь сравнения (1) и сокращая на

$$1\cdot 2\dots p_1=r_1 r_2\dots r_{p_1},$$

получим $a^{\frac{p-1}{2}}\equiv\varepsilon_1\varepsilon_2\dots\varepsilon_{p_1}\pmod p$, откуда (b) имеем

$$\left(\frac{a}{p}\right)=\varepsilon_1\varepsilon_2\dots\varepsilon_{p_1}.\qquad(2)$$

i. Найденному выражению символа Лежандра придадим более законченный вид. Имеем

$$\left[\frac{2ax}{p}\right]=\left[2\left[\frac{ax}{p}\right]+2\left\{\frac{ax}{p}\right\}\right]=2\left[\frac{ax}{p}\right]+\left[2\left\{\frac{ax}{p}\right\}\right],$$

что будет чётным или нечётным, в зависимости от того, будет ли наименьший неотрицательный вычет числа ax меньше или больше $\frac{1}{2}p$, т. е. будет ли $\varepsilon_x=1$ или $\varepsilon_x=-1$. Отсюда, очевидно,

$$\varepsilon_x=(-1)^{\left[\frac{2ax}{p}\right]},$$

и потому из (2) находим

$$\left(\frac{a}{p}\right)=(-1)^{\sum_{x=1}^{p_1}\left[\frac{2ax}{p}\right]},$$

j. Предполагая a нечётным, преобразуем последнее равенство. Имеем ($a+p$ — чётное)

$$\left(\frac{2a}{p}\right)=\left(\frac{2a+2p}{p}\right)=\left(\frac{4\frac{a+p}{2}}{p}\right)=\left(\frac{\frac{a+p}{2}}{p}\right)=$$

$$=(-1)^{\sum_{x=1}^{p_1}\left[\frac{(a+p)x}{p}\right]}=(-1)^{\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]+\sum_{x=1}^{p_1}x},$$

откуда

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right)=(-1)^{\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]+\frac{p^2-1}{8}}. \qquad (3)$$

Формула (3) позволит нам вывести два весьма важных свойства символа Лежандра.

k. $$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

Следует из формулы (3) при $a=1$.

Так как, далее,

$$\frac{(8m\pm1)^2-1}{8}=8m^2\pm2m \text{ чётное},$$

а

$$\frac{(8m\pm3)^2-1}{8}=8m^2\pm6m+1 \text{ нечётное},$$

то отсюда следует, что 2 будет квадратичным вычетом простых чисел формы $8m\pm1$ ($8m+1$, $8m+7$) и квадратичным невычетом простых чисел формы

$$8m\pm3 \quad (8m+3,\ 8m+5).$$

l. *Если p и q — простые нечётные, то* (*закон взаимности квадратичных вычетов*)

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

Так как $\frac{p-1}{2}\cdot\frac{q-1}{2}$ будет нечётным лишь в случае, когда оба числа p и q будут формы $4m+3$, и чётным, если хоть одно из этих чисел будет формы $4m+1$, то указанное свойство можно формулировать так:

Если оба числа p и q формы $4m+3$, то

$$\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right);$$

если же хоть одно из них формы $4m+1$, то

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right).$$

Для доказательства заметим, что ввиду k формула (3) принимает вид

$$\left(\frac{a}{p}\right)=(-1)^{\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]}. \qquad (4)$$

Полагая теперь $\frac{q-1}{2}=q_1$, рассмотрим p_1q_1 пар чисел, получаемых, когда в выражениях qx, py числа x и y независимо друг от друга пробегают системы значений

$$x=1,\ 2,\ \ldots,\ p_1, \quad y=1,\ 2,\ \ldots,\ q_1.$$

Никогда не может быть $qx=py$, потому что из этого равенства следовало бы, что py кратно q, что ввиду $(p, q)=(y, q)=1$ (так как $0<y<q$) невозможно. Поэтому мы можем положить $p_1q_1=S_1+S_2$, где S_1 — число пар с $qx<py$ и S_2 — число пар с $py<qx$.

Очевидно, S_1 есть также число пар с $x<\frac{p}{q}y$. Здесь при данном y можно брать $x=1,\ 2,\ \ldots,\ \left[\frac{p}{q}y\right]$. (Ввиду $\frac{p}{q}y\leqslant\frac{p}{q}q_1<\frac{p}{2}$ имеем $\left[\frac{p}{q}y\right]\leqslant p_1$.) Следовательно,

$$S_1=\sum_{y=1}^{q_1}\left[\frac{p}{q}y\right].$$

Аналогичным путём убедимся, что

$$S_2 = \sum_{x=1}^{p_1} \left[\frac{q}{p} x\right].$$

Но тогда равенство (4) даёт нам

$$\left(\frac{p}{q}\right) = (-1)^{S_1}, \quad \left(\frac{q}{p}\right) = (-1)^{S_2},$$

поэтому

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S_1+S_2} = (-1)^{p_1 q_1},$$

откуда и следует отмеченное свойство.

§ 3. Символ Якоби

a. Чтобы сделать вычисление символа Лежандра более быстрым, рассматривают более общий *символ Якоби*. Пусть P — нечётное, большее единицы, и $P = p_1 p_2 \dots p_r$ — разложение его на простые сомножители (среди них могут быть и равные). Пусть, далее, $(a, P) = 1$. Тогда символ Якоби $\left(\frac{a}{P}\right)$ определяется равенством

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_r}\right).$$

Известные свойства символа Лежандра дают возможность установить аналогичные свойства и для символа Якоби.

b. *Если* $a \equiv a_1 \pmod P$, *то* $\left(\frac{a}{P}\right) = \left(\frac{a_1}{P}\right)$.

Действительно,

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_r}\right) = \\ = \left(\frac{a_1}{p_1}\right)\left(\frac{a_1}{p_2}\right)\dots\left(\frac{a_1}{p_r}\right) = \left(\frac{a_1}{P}\right),$$

потому что a, будучи сравнимо с a_1 по модулю P, будет сравнимо с a_1 и по модулям $p_1, p_2, \dots, p_r$, которые являются делителями P.

c. $\left(\frac{1}{P}\right) = 1$.

В самом деле,

$$\left(\frac{1}{P}\right) = \left(\frac{1}{p_1}\right)\left(\frac{1}{p_2}\right)\dots\left(\frac{1}{p_r}\right) = 1.$$

d. $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$.

Чтобы убедиться в этом, заметим, что

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\dots\left(\frac{-1}{p_r}\right) = \\ = (-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+\dots+\frac{p_r-1}{2}}; \qquad (1)$$

но

$$\frac{P-1}{2} = \frac{p_1 p_2 \dots p_r - 1}{2} = \\ = \frac{\left(1+2\frac{p_1-1}{2}\right)\left(1+2\frac{p_2-1}{2}\right)\dots\left(1+2\frac{p_r-1}{2}\right)-1}{2} = \\ = \frac{p_1-1}{2}+\frac{p_2-1}{2}+\dots+\frac{p_r-1}{2}+2N,$$

ввиду чего из формулы (1) выводим

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}.$$

e. $\left(\frac{ab\dots l}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right)\dots\left(\frac{l}{P}\right)$.

Действительно,

$$\left(\frac{ab\dots l}{P}\right) = \left(\frac{ab\dots l}{p_1}\right)\dots\left(\frac{ab\dots l}{p_r}\right) = \\ = \left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\dots\left(\frac{l}{p_1}\right)\dots\left(\frac{a}{p_r}\right)\left(\frac{b}{p_r}\right)\dots\left(\frac{l}{p_r}\right);$$

собирая символы с одинаковыми числителями, мы и получим утверждаемое свойство. Отсюда следствие:

$$\left(\frac{ab^2}{P}\right)=\left(\frac{a}{P}\right).$$

f. $\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}$.

Действительно,

$$\left(\frac{2}{P}\right)=\left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_r}\right)=$$
$$=(-1)^{\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\ldots+\frac{p_r^2-1}{8}}. \qquad (2)$$

Но

$$\frac{P^2-1}{8}=\frac{p_1^2p_2^2\ldots p_r^2-1}{8}=$$
$$=\frac{\left(1+8\frac{p_1^2-1}{8}\right)\left(1+8\frac{p_2^2-1}{8}\right)\cdots\left(1+8\frac{p_r^2-1}{8}\right)-1}{8}=$$
$$=\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\ldots+\frac{p_r^2-1}{8}+2N,$$

ввиду чего из формулы (2) выводим

$$\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}.$$

g. *Если P и Q — положительные нечётные взаимно простые, то*

$$\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right).$$

Действительно, пусть $Q=q_1q_2\ldots q_s$ есть разложение Q на простые сомножители (среди них опять-таки могут

быть равные). Имеем

$$\left(\frac{Q}{P}\right)=\left(\frac{Q}{p_1}\right)\left(\frac{Q}{p_2}\right)\cdots\left(\frac{Q}{p_r}\right)=\prod_{\alpha=1}^{r}\prod_{\beta=1}^{s}\left(\frac{q_\beta}{p_\alpha}\right)=$$
$$=(-1)^{\sum_{\alpha=1}^{r}\sum_{\beta=1}^{s}\frac{p_\alpha-1}{2}\cdot\frac{q_\beta-1}{2}}\prod_{\alpha=1}^{r}\prod_{\beta=1}^{s}\left(\frac{p_\alpha}{q_\beta}\right)=$$
$$=(-1)^{\left(\sum_{\alpha=1}^{r}\frac{p_\alpha-1}{2}\right)\left(\sum_{\beta=1}^{s}\frac{q_\beta-1}{2}\right)}\left(\frac{P}{Q}\right).$$

Но, подобно тому, как в d, находим

$$\frac{P-1}{2}=\sum_{\alpha=1}^{r}\frac{p_\alpha-1}{2}+2N,\quad \frac{Q-1}{2}=\sum_{\beta=1}^{s}\frac{q_\beta-1}{2}+2N_1,$$

ввиду чего последняя формула даёт

$$\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right).$$

Пример. В качестве примера на вычисление символа Лежандра (при этом будем рассматривать его как частный случай символа Якоби) исследуем, имеет ли решение сравнение

$$x^2\equiv 219 \pmod{383}.$$

Имеем (применяя последовательно свойства **g**, **b**, следствие **e**, **g**, **b**, **e**, **f**, **g**, **b**, **d**):

$$\left(\frac{219}{383}\right)=-\left(\frac{383}{219}\right)=-\left(\frac{164}{219}\right)=-\left(\frac{41}{219}\right)=$$
$$=-\left(\frac{219}{41}\right)=-\left(\frac{14}{41}\right)=-\left(\frac{2}{41}\right)\left(\frac{7}{41}\right)=$$
$$=-\left(\frac{7}{41}\right)=-\left(\frac{41}{7}\right)=-\left(\frac{-1}{7}\right)=1;$$

следовательно, рассмотренное сравнение имеет два решения.

§ 4. Случай составного модуля.

a. Сравнения второй степени по составному модулю исследуются и решаются согласно общим указаниям § 5, гл. IV.

b. Начнём со сравнения вида

$$x^2 \equiv a \pmod{p^\alpha}; \quad \alpha > 0, \quad (a, p) = 1, \tag{1}$$

где p — простое нечётное.

Полагая $f(x) = x^2 - a$, будем иметь $f'(x) = 2x$, и если $x \equiv x_1 \pmod p$ есть решение сравнения

$$x^2 \equiv a \pmod p, \tag{2}$$

то ввиду $(a, p) = 1$ также $(x_1, p) = 1$, а так как p нечётное, то $(2x_1, p) = 1$, т. е. $f'(x_1)$ не делится на p. Поэтому к разысканию решений сравнения (1) можно применить рассуждения b, § 5, гл. IV, причём каждое решение сравнения (2) даст одно решение сравнения (1). Из сказанного выводим, что

Сравнение (1) *имеет два решения или же ни одного, в зависимости от того, будет ли число* a *квадратичным вычетом или же невычетом по модулю* p.

c. Теперь рассмотрим сравнение

$$x^2 \equiv a \pmod{2^\alpha}; \quad \alpha > 0, \quad (a, 2) = 1. \tag{3}$$

Здесь $f'(x_1) = 2x_1$ делится на 2, и потому рассуждения b, § 5, гл. IV неприменимы; они должны быть видоизменены следующим образом:

d. Если сравнение (3) разрешимо, то ввиду $(a, 2) = 1$ имеем $(x, 2) = 1$, т. е. $x = 1 + 2t$, где t — целое. Сравнение (3) принимает вид

$$1 + 4t(t+1) \equiv a \pmod{2^\alpha}.$$

Но одно из чисел t, $t+1$ — чётное, поэтому $4t(t+1)$ кратно 8. Следовательно, для разрешимости последнего сравнения, а вместе с тем и сравнения (3) необходимо

$$a \equiv 1 \pmod 4 \text{ при } \alpha = 2; \quad a \equiv 1 \pmod 8 \text{ при } \alpha \geqslant 3. \tag{4}$$

e. В случаях, когда условия (4) не нарушены, рассмотрим вопрос о разыскании решений и их числе.

Для случаев $\alpha \leqslant 3$ ввиду d сравнению удовлетворяют все нечётные числа. Поэтому сравнение $x^2 \equiv a \pmod 2$ имеет одно решение: $x \equiv 1 \pmod 2$, сравнение $x^2 \equiv a \pmod 4$ имеет два решения: $x \equiv 1; 3 \pmod 4$, сравнение $x^2 \equiv a \pmod 8$ имеет четыре решения: $x \equiv 1; 3; 5; 7 \pmod 8$.

Для рассмотрения случаев $\alpha = 4, 5, \ldots$ все нечётные числа полезно объединить в две арифметические прогрессии:

$$x = \pm(1 + 4t_3) \tag{5}$$

$$(1 + 4t_3 \equiv 1 \pmod 4; \quad -1 - 4t_3 \equiv -1 \equiv 3 \pmod 4).$$

Посмотрим, какие из чисел (5) удовлетворяют сравнению $x^2 \equiv a \pmod{16}$. Находим

$$(1 + 4t_3)^2 \equiv a \pmod{16}, \quad t_3 \equiv \frac{a-1}{8} \pmod 2,$$

$$t_3 = t_3' + 2t_4, \quad x = \pm(1 + 4t_3' + 8t_4) = \pm(x_4 + 8t_4).$$

Посмотрим, какие из последних чисел удовлетворяют сравнению $x^2 \equiv a \pmod{32}$. Находим

$$(x_4 + 8t_4)^2 \equiv a \pmod{32}, \quad t_4 = t_4' + 2t_5, \quad x = \pm(x_5 + 16t_5),$$

и т. д. Таким путём убедимся, что при любом $\alpha > 3$ значения x, удовлетворяющие сравнению (3), представятся в форме

$$x = \pm(x_\alpha + 2^{\alpha-1} t_\alpha).$$

Эти значения x образуют четыре различных решения сравнения (3)

$$x \equiv x_\alpha; \quad x_\alpha + 2^{\alpha-1}; \quad -x_\alpha; \quad -x_\alpha - 2^{\alpha-1} \pmod{2^\alpha}$$

(по модулю 4 два первых сравнимы с 1, а два последних сравнимы с -1).

Пример. Сравнение

$$x^2 \equiv 57 \pmod{64} \tag{6}$$

ввиду $57 \equiv 1 \pmod 8$ имеет четыре решения. Представляя

x в форме $x = \pm(1 + 4t_3)$, находим

$$(1+4t_3)^2 \equiv 57 \pmod{16}, \quad 8t_3 \equiv 56 \pmod{16},$$
$$t_3 \equiv 1 \pmod 2, \quad t_3 = 1 + 2t_4; \quad x = \pm(5 + 8t_4),$$
$$(5+8t_4)^2 \equiv 57 \pmod{32}, \quad 5 \cdot 16t_4 \equiv 32 \pmod{32},$$
$$t_4 \equiv 0 \pmod 2, \quad t_4 = 2t_5, \quad x = \pm(5 + 16t_5),$$
$$(5+16t_5)^2 \equiv 57 \pmod{64}, \quad 5 \cdot 32t_5 \equiv 32 \pmod{64},$$
$$t_5 \equiv 1 \pmod 2, \quad t_5 = 1 + 2t_6, \quad x = \pm(21 + 32t_6).$$

Поэтому решения сравнения (6) будут:

$$x \equiv \pm 21; \pm 53 \pmod{64}.$$

f. Из **c**, **d** и **e** следует:
Для сравнения

$$x^2 \equiv a \pmod{2^\alpha}; \quad (a, 2) = 1$$

необходимыми условиями разрешимости будут: $a \equiv 1 \pmod 4$ *при* $\alpha = 2$, $a \equiv 1 \pmod 8$ *при* $\alpha \geqslant 3$. *Если эти условия не нарушены, число решений будет*: 1 *при* $\alpha = 1$; 2 *при* $\alpha = 2$; 4 *при* $\alpha \geqslant 3$.

g. Из **b**, **f** и **a**, § 5, гл. IV следует:
Для сравнения общего вида

$$x^2 \equiv a \pmod m; \quad m = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}; \quad (a, m) = 1$$

необходимыми условиями разрешимости будут:

$$a \equiv 1 \pmod 4 \text{ при } \alpha = 2, \quad a \equiv 1 \pmod 8 \text{ при } \alpha \geqslant 3,$$
$$\left(\frac{a}{p_1}\right) = 1, \quad \left(\frac{a}{p_2}\right) = 1, \quad \dots, \quad \left(\frac{a}{p_k}\right) = 1.$$

Если ни одно из этих условий не нарушено, число решений будет: 2^k *при* $\alpha = 0$ *и при* $\alpha = 1$; 2^{k+1} *при* $\alpha = 2$; 2^{k+2} *при* $\alpha \geqslant 3$.

Вопросы к главе V.

Буквою p здесь всегда обозначаем простое нечётное число.

1. Доказать, что разыскание решений сравнения вида

$$ax^2 + bx + c \equiv 0 \pmod m, \qquad (2a, m) = 1$$

сводится к разысканию решений сравнения вида $x^2 \equiv q \pmod m$.

2, a. Пользуясь **e**, § 1, найти решения сравнения (в случае его возможности)

$$x^2 \equiv a \pmod p; \qquad p = 4m + 3.$$

b. Пользуясь **b** и **k**, § 2, указать способ разыскания решений сравнений вида

$$x^2 \equiv a \pmod p; \qquad p = 8m + 5.$$

c. Указать возможно более простой способ разыскания решений сравнений вида

$$x^2 \equiv a \pmod p; \qquad p = 8m + 1$$

в случае, когда известен некоторый квадратичный невычет N по модулю p.

d. Пользуясь теоремой Вильсона, доказать, что решения сравнения

$$x^2 + 1 \equiv 0 \pmod p; \qquad p = 4m + 1$$

будут

$$x \equiv \pm 1 \cdot 2 \dots 2m \pmod p$$

3, a. Доказать, что сравнение

$$x^2 + 1 \equiv 0 \pmod p \tag{1}$$

разрешимо тогда и только тогда, когда p имеет вид $4m+1$; сравнение

$$x^2 + 2 \equiv 0 \pmod p \tag{2}$$

разрешимо тогда и только тогда, когда p имеет вид $8m + 1$ или $8m + 3$; сравнение

$$x^2 + 3 \equiv 0 \pmod p \tag{3}$$

разрешимо тогда и только тогда, когда p имеет вид $6m + 1$.

b. Доказать бесконечность числа простых чисел вида $4m + 1$.

c. Доказать бесконечность числа простых чисел вида $6m + 1$.

4. Пусть, разбивая числа $1, 2, \dots, p-1$ на две совокупности, вторая из которых содержит не менее одного числа, имеем: произведение двух чисел одной совокупности сравнимо по модулю p с числом первой совокупности, а произведение двух чисел различных совокупностей сравнимо по модулю p с числом второй совокупности. Доказать, что это будет тогда и только тогда, когда первая совокупность состоит из квадратичных вычетов, а вторая — из квадратичных невычетов по модулю p.

5, a. Вывести теорию сравнений вида

$$x^2 \equiv a \pmod{p^\alpha}; \qquad (a, p) = 1,$$

представляя a и x в системе исчисления с основанием p.

b. Вывести теорию сравнений вида

$$x^2 \equiv a \pmod{2^\alpha}; \qquad (a, 2)=1,$$

представляя a и x в системе исчисления с основанием 2.

6. Доказать, что решения сравнения

$$x^2 \equiv a \pmod{p^\alpha}; \qquad (a, p)=1$$

будут $x \equiv \pm PQ' \pmod{p^\alpha}$, где

$$P=\frac{(z+\sqrt{a})^\alpha+(z-\sqrt{a})^\alpha}{2}, \qquad Q=\frac{(z+\sqrt{a})^\alpha-(z-\sqrt{a})^\alpha}{2\sqrt{a}},$$

$$z^2 \equiv a \pmod{p}, \qquad QQ' \equiv 1 \pmod{p^\alpha}.$$

7. Указать способ решения сравнения $x^2 \equiv 1 \pmod{m}$, основанный на том обстоятельстве, что указанное сравнение равносильно такому: $(x-1)(x+1) \equiv 0 \pmod{m}$.

8. Пусть $\left(\frac{a}{p}\right)=0$ при $(a, p)=p$.

a. При $(k, p)=1$ доказать, что

$$\sum_{x=0}^{p-1}\left(\frac{x(x+k)}{p}\right)=-1.$$

b. Пусть каждое из чисел ε и η имеет одно из значений ± 1, T — число пар x, $x+1$, где $x=1, 2, \ldots, p-2$, с условием $\left(\frac{x}{p}\right)=\varepsilon$, $\left(\frac{x+1}{p}\right)=\eta$. Доказать, что

$$T=\frac{1}{4}\left(p-2-\varepsilon\left(\frac{-1}{p}\right)-\eta-\varepsilon\eta\right).$$

c. Пусть $(k, p)=1$,

$$S=\sum_x\sum_y\left(\frac{xy+k}{p}\right),$$

где x и y пробегают возрастающие последовательности, составленные соответственно из X и Y вычетов полной системы по модулю p. Доказать, что

$$|S|<\sqrt{2XYp}.$$

Для доказательства следует воспользоваться неравенством

$$S^2 \leqslant X\sum_x\left|\sum_y\left(\frac{xy+k}{p}\right)\right|^2.$$

d. Пусть Q — целое, $1<Q<p$,

$$S=\sum_{x=0}^{p-1}S_x^2; \qquad S_x=\sum_{z=0}^{Q-1}\left(\frac{x+z}{p}\right).$$

α) Доказать, что $S=(p-Q)Q$.

β) Пусть λ — постоянное; $0<\lambda<1$. Доказать, что число T чисел ряда $x=0, 1, \ldots, p-1$, для которых не выполняется условие $S_x \leqslant Q^{0,5+0,5\lambda}$, удовлетворяет условию $T \leqslant pQ^{-\lambda}$.

γ) Пусть $p>25$, M — целое. Доказать, что в ряде

$$M, M+1, \ldots, M+3[\sqrt{p}]-1$$

имеется квадратичный невычет по модулю p.

9, a. Доказать, что число представлений целого $m>1$ в виде

$$m=x^2+y^2, \quad (x, y)=1, \quad x>0, y>0 \qquad (1)$$

равно числу решений сравнения

$$z^2+1 \equiv 0 \pmod{m}. \qquad (2)$$

Для доказательства, положив $\tau=\sqrt{m}$, воспользоваться представлением $\alpha=\frac{z}{m}$ согласно теореме вопроса 4, b, гл. I, и рассмотреть сравнение, получаемое почленным умножением (2) на Q^2.

b. Пусть a — одно из чисел 2 и 3. Доказать, что число представлений простого p с условием $p>a$ в виде

$$p=x^2+ay^2, \quad x>0, \quad y>0 \qquad (3)$$

равно половине числа решений сравнения

$$z^2+a \equiv 0 \pmod{p}. \qquad (4)$$

c. Пусть p имеет вид $4m+1$, $(k, p)=1$.

$$S(k)=\sum_{x=0}^{p-1}\left(\frac{x(x^2+k)}{p}\right).$$

Доказать, что (Д. С. Горшков)

α) $S(k)$ — чётное число.

β) $S(kt^2)=\left(\frac{t}{p}\right)S(k)$.

γ) При $\left(\frac{r}{p}\right)=1$, $\left(\frac{n}{p}\right)=-1$ имеем (ср. вопрос a)

$$p=\left(\frac{1}{2}S(r)\right)^2+\left(\frac{1}{2}S(n)\right)^2.$$

10. Пусть D — целое положительное, не являющееся квадратом целого числа. Доказать, что:

a. Если при данном целом k уравнению

$$x^2 - Dy^2 = k$$

удовлетворяют две пары целых $x = x_1$, $y = y_1$ и $x = x_2$, $y = y_2$, то уравнению

$$X^2 - DY^2 = k^2$$

удовлетворяют целые X, Y, определяемые равенством (знак $\pm$ выбирается произвольно)

$$X + Y\sqrt{D} = (x_1 + y_1\sqrt{D})(x_2 \pm y_2\sqrt{D}).$$

b. Уравнение (уравнение Пелля)

$$x^2 - Dy^2 = 1 \tag{1}$$

разрешимо в целых положительных x, y.

c. Если x_0, y_0 — пара положительных x, y с наименьшим x (или, что равносильно, с наименьшим $x + y\sqrt{D}$), удовлетворяющая уравнению (1), то все пары положительных x, y, удовлетворяющие этому уравнению, определяются равенством

$$x + y\sqrt{D} = (x_0 + y_0\sqrt{D})^r; \quad r = 1, 2, \ldots \tag{2}$$

11, a. Пусть a — целое,

$$U_{a,p} = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e^{2\pi i \frac{ax}{p}}.$$

α) При $(a, p) = 1$ доказать, что $|U_{a,p}| = \sqrt{p}$.

Для доказательства следует сумму $U_{a,p}$ умножить на сопряжённую, получаемую заменой i на $-i$. Обозначая буквами x_1 и x переменные суммирования основной и сопряжённой сумм, следует собрать вместе те члены произведения, где при данном t

$$x_1 \equiv xt \pmod{p},$$

или же

$$x_1 \equiv x + t \pmod{p}.$$

β) Доказать, что

$$\left(\frac{a}{p}\right) = \frac{U_{a,p}}{U_{1,p}}$$

b. Пусть $m > 2$, $(a, m) = 1$,

$$S_{a,m} = \sum_{x=0}^{m-1} e^{2\pi i \frac{ax^2}{m}}.$$

α) Доказать, что $S_{a,p} = U_{a,p}$ (вопрос **a**).

β) Из теорем вопросов α) и **a**, α) следует, что $S_{a,p} = \sqrt{p}$. Доказать следующий более общий результат:

$$|S_{a,m}| = \sqrt{m}, \quad \text{если } m \equiv 1 \pmod 2,$$

$$|S_{a,m}| = 0, \quad \text{если } m \equiv 2 \pmod 4,$$

$$|S_{a,m}| = \sqrt{2m}, \quad \text{если } m \equiv 0 \pmod 4.$$

γ) Пусть $m > 1$, $(2A, m) = 1$, α = любое целое число. Доказать, что

$$\left| \sum_{x=0}^{m-1} e^{2\pi i \frac{Ax^2 + \alpha x}{m}} \right| = \sqrt{m}.$$

12, a. Пусть m — целое, превосходящее 1, M и Q — целые, $0 \leqslant M < M + Q \leqslant m$, $\sum_z$ обозначает сумму, распространённую по z на заданную совокупность целых чисел, а $\sum_z'$ обозначает сумму, распространённую по z лишь на числа этой совокупности, сравнимые по модулю m с числами

$$M, M+1, \ldots, M+Q-1.$$

Пусть, далее, функция $\Phi(z)$ такова, что при некотором Δ и любом $a = 1, 2, \ldots, m-1$ имеем

$$\left| \sum_z \Phi(z)\, e^{2\pi i \frac{az}{m}} \right| \leqslant \Delta.$$

Доказать, что

$$\sum_z' \Phi(z) = \frac{Q}{m} \sum_z \Phi(z) + \vartheta\Delta(\ln m - \delta),$$

где $|\vartheta| < 1$, $\delta > 0$ всегда, $\delta > \frac{1}{2}$ при $m \geqslant 12$, $\delta > 1$ при $m \geqslant 60$.

b. Пусть M и Q — целые, $0 < M < M + Q \leqslant p$.

α) Доказать, что

$$\left| \sum_{x=M}^{M+Q-1} \left(\frac{x}{p}\right) \right| < \sqrt{p} \ln p$$

β) Пусть R — число квадратичных вычетов и N — число квадратичных невычетов в ряде $M, M+1, \ldots, M+Q-1$. Доказать, что

$$R=\frac{1}{2}Q+\frac{\theta}{2}\sqrt{p}\ln p, \qquad N=\frac{1}{2}Q-\frac{\theta}{2}\sqrt{p}\ln p; \quad |\theta|<1.$$

γ) Формулы вопроса β) вывести, пользуясь теоремой вопроса 11, b, β) и теоремой вопроса a.

δ) Пусть $m \geqslant 60$, $(2A, m)=1$, M_0 и Q_0 — целые, $0<M_0<M_0+Q_0 \leqslant m$. Доказать, что

$$\left|\sum_{x=M_0}^{M_0+Q_0-1} e^{2\pi i\frac{Ax^2}{m}}\right| < \sqrt{m}\ln m.$$

ε) Пусть $p>60$, $(A, p)=1$, M_0 и Q_0 — целые, $0<M_0<M_0+Q_0 \leqslant p$ и T обозначает число чисел ряда Ax^2; $x=M_0, M_0+1, \ldots, M_0+Q_0-1$, сравнимых по модулю p с числами ряда $M, M+1, \ldots, M+Q-1$. Доказать, что

$$T=\frac{Q_0Q}{p}+\theta\sqrt{p}(\ln p)^2.$$

c. Формулы вопроса b, β) вывести, рассматривая сумму

$$\sum_{a=0}^{p-1}\sum_{\alpha=1}^{p-1}\sum_{x=M}^{M+Q-1}\sum_{y=M}^{M+Q-1}\left(\frac{\alpha}{p}\right)e^{2\pi i\frac{a(x-\alpha y)}{p}}.$$

Численные примеры к главе V.

1, a. Среди вычетов приведённой системы по модулю 23 указать квадратичные вычеты.

b. Среди вычетов приведённой системы по модулю 37 указать квадратичные невычеты.

2, a. Применяя e, § 1, указать число решений сравнений

α) $x^2 \equiv 3 \pmod{31}$; β) $x^2 \equiv 2 \pmod{31}$.

b. Указать число решений сравнений:

α) $x^2 \equiv 5 \pmod{73}$; β) $x^2 \equiv 3 \pmod{73}$.

3, a. Вычисляя символ Якоби, указать число решений сравнений

α) $x^2 \equiv 226 \pmod{563}$; β) $x^2 \equiv 429 \pmod{563}$.

b. Указать число решений сравнений

α) $x^2 \equiv 3766 \pmod{5987}$; β) $x^2 \equiv 3149 \pmod{5987}$.

4, a. Применяя способы вопросов 2, a; 2, b; 2, c, решить сравнения:

α) $x^2 \equiv 5 \pmod{19}$; β) $x^2 \equiv 5 \pmod{29}$; γ) $x^2 \equiv 2 \pmod{97}$.

b. Решить сравнения:

α) $x^2 \equiv 2 \pmod{311}$; β) $x^2 \equiv 3 \pmod{277}$; γ) $x^2 \equiv 11 \pmod{353}$.

5, a. Решить сравнение $x^2 \equiv 59 \pmod{125}$ способами

α) b, § 4; β) вопроса 5, a; γ) вопроса 6.

b. Решить сравнение $x^2 \equiv 91 \pmod{243}$.

6, a. Решить сравнение $x^2 \equiv 41 \pmod{64}$ способами:

α) c, § 4; β) вопроса 5, b.

b. Решить сравнение $x^2 \equiv 145 \pmod{256}$.

ГЛАВА ШЕСТАЯ.

ПЕРВООБРАЗНЫЕ КОРНИ И ИНДЕКСЫ.

§ 1. Общие теоремы.

a. При $(a, m) = 1$ существуют положительные γ с условием $a^\gamma \equiv 1 \pmod m$, например (теорема Эйлера) $\gamma = \varphi(m)$. Наименьшее из них называется: *показатель, которому a принадлежит по модулю m.*

b. *Если a по модулю m принадлежит показателю δ, то числа $1 = a^0, a^1, \ldots, a^{\delta-1}$ по модулю m несравнимы.*

Действительно, из $a^l \equiv a^k \pmod m$, $0 \leqslant k < l < \delta$ следовало бы $a^{l-k} \equiv 1 \pmod m$; $0 < l-k < \delta$, что противоречит определению δ.

c. *Если a по модулю m принадлежит показателю δ, то $a^\gamma \equiv a^{\gamma'} \pmod m$ тогда и только тогда, когда $\gamma \equiv \gamma' \pmod \delta$; в частности (при $\gamma' = 0$), $a^\gamma \equiv 1 \pmod m$ тогда и только тогда, когда γ делится на δ.*

Действительно, пусть r и r_1 — наименьшие неотрицательные вычеты чисел γ и γ' по модулю δ; тогда при некоторых q и q_1 имеем $\gamma = \delta q + r$, $\gamma' = \delta q_1 + r_1$. Отсюда и из $a^\delta \equiv 1 \pmod m$ следует

$$a^\gamma = (a^\delta)^q a^r \equiv a^r \pmod m,$$

$$a^{\gamma'} = (a^\delta)^{q_1} a^{r_1} \equiv a^{r_1} \pmod m.$$

Поэтому $a^\gamma \equiv a^{\gamma_1} \pmod m$ тогда и только тогда, когда $a^r \equiv a^{r_1} \pmod m$, т. е. (b), когда $r = r_1$.

d. Из $a^{\varphi(m)} \equiv 1 \pmod m$ и из c ($\gamma' = 0$) следует, что $\varphi(m)$ делится на δ. Таким образом *показатели, которым числа принадлежат по модулю m, суть делители* $\varphi(m)$. Наибольший из этих делителей есть само $\varphi(m)$. Числа, принадлежащие показателю $\varphi(m)$ (если такие существуют), называются *первообразными корнями по модулю m.*

§ 2. Первообразные корни по модулям p^α и $2p^\alpha$.

a. Пусть p — простое нечётное и $\alpha > 1$. Докажем существование первообразных корней по модулям p^α и $2p^\alpha$.

b. *Если x по модулю m принадлежит показателю ab, то x^a принадлежит показателю b.*

Действительно, пусть x^a принадлежит показателю δ. Тогда $(x^a)^\delta \equiv 1 \pmod m$, откуда $x^{a\delta} \equiv 1 \pmod m$; следовательно (c, § 1) $a\delta$ делится на ab, т. е. δ делится на b. С другой стороны, $x^{ab} \equiv 1 \pmod m$, откуда $(x^a)^b \equiv 1 \pmod m$; следовательно (c, § 1) b делится на δ. Поэтому $\delta = b$.

c. *Если x по модулю m принадлежит показателю a, а y — показателю b, причём $(a, b) = 1$, то xy принадлежит показателю ab.*

Действительно, пусть xy принадлежит показателю δ. Тогда $(xy)^\delta \equiv 1 \pmod m$. Отсюда $x^{b\delta} y^{b\delta} \equiv 1 \pmod m$ и (c, § 1) $x^{b\delta} \equiv 1 \pmod m$. Поэтому (c, § 1) $b\delta$ делится на a, и ввиду $(b, a) = 1$ δ делится на a. Так же находим, что δ делится на b. Делясь же на a и на b, ввиду $(a, b) = 1$ δ делится и на ab. С другой стороны, из $(xy)^{ab} \equiv 1 \pmod m$ следует (c, § 1), что ab делится на δ. Поэтому $\delta = ab$.

d. *Существуют первообразные корни по модулю p.*

Действительно, пусть τ — общее наименьшее кратное всех тех показателей

$$\delta_1, \delta_2, \ldots, \delta_r, \tag{1}$$

каждому из которых по модулю p принадлежит хотя бы одно число ряда $1, 2, \ldots, p-1$, и пусть $\tau = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k}$ — каноническое разложение числа τ; тогда при каждом s среди чисел (1) существует некоторое δ, делящееся на $q_s^{\alpha_s}$ и тем самым представимое в форме $\delta = a q_s^{\alpha_s}$. Если x — число, принадлежащее показателю δ, то, согласно b, $x_s = x^a$ принадлежит показателю $q_s^{\alpha_s}$. Сказанное относится

к $s=1, 2, \ldots, k$; согласно с число $g=x_1x_2\ldots x_k$ принадлежит показателю $q_1^{\alpha_1}q_2^{\alpha_2}\ldots q_k^{\alpha_k}=\tau$.

Но поскольку показатели (1) суть делители числа τ, то все числа $1, 2, \ldots, p-1$ удовлетворяют (с, § 1) сравнению $x^\tau \equiv 1 \pmod p$. Значит (с, § 4, гл. IV), $p-1 \leqslant \tau$. Но τ — делитель числа $p-1$. Поэтому $\tau = p-1$, т. е. g — первообразный корень.

с. *Пусть g — первообразный корень по модулю p. Можно указать t с условием, что u, определяемое равенством $(g+pt)^{p-1}=1+pu$, не делится на p. Соответствующее $g+pt$ будет первообразным корнем по модулю p^α при любом $\alpha>1$.*

Действительно, имеем

$$g^{p-1}=1+pT_0,$$
$$(g+pt)^{p-1}=1+p(T_0-g^{p-2}t+pT)=1+pu, \qquad (2)$$

где, одновременно с t, u пробегает полную систему вычетов по модулю p. Поэтому можно указать t с условием, что u не делится на p. При указанном t из (2) выводим также

$$\left.\begin{aligned}(g+pt)^{p(p-1)}&=(1+pu)^p=1+p^2u_2,\\ (g+pt)^{p^2(p-1)}&=(1+p^2u_2)^p=1+p^3u_3,\\ &\cdots\cdots\cdots\cdots\cdots\end{aligned}\right\} \qquad (3)$$

где $u_2, u_3, \ldots$ не делятся на p.

Пусть $g+pt$ по модулю p^α принадлежит показателю δ. Тогда

$$(g+pt)^\delta \equiv 1 \pmod{p^\alpha}. \qquad (4)$$

Отсюда $(g+pt)^\delta \equiv 1 \pmod p$; следовательно, δ кратно $p-1$, а так как δ делит $\varphi(p^\alpha)=p^{\alpha-1}(p-1)$, то $\delta=p^{r-1}(p-1)$, где r — одно из чисел $1, 2, \ldots, \alpha$. Заменяя левую часть сравнения (4) её выражением из соответствующего из равенств (2) и (3), получим ($u=u_1$)

$$1+p^ru_r \equiv 1 \pmod{p^\alpha},\ p^r \equiv 0 \pmod{p^\alpha},\ r=\alpha,\ \delta=\varphi(p^\alpha),$$

т. е. $g+pt$ — первообразный корень по модулю p^α.

f. *Пусть $\alpha \geqslant 1$ и g_1 — первообразный корень по модулю p^α. Нечётное из чисел g_1 и g_1+p^α будет первообразным корнем по модулю $2p^\alpha$.*

Действительно, всякое нечётное x, удовлетворяющее одному из сравнений $x^\gamma \equiv 1 \pmod{p^\alpha}$ и $x^\gamma \equiv 1 \pmod{2p^\alpha}$, очевидно, удовлетворяет и другому. Поэтому ввиду $\varphi(p^\alpha)=\varphi(2p^\alpha)$ всякое нечётное x, являющееся первообразным корнем по одному из модулей p^α и $2p^\alpha$, является первообразным корнем и по другому. Но из двух первообразных корней g_1 и g_1+p^α по модулю p^α один — непременно нечётный; он, следовательно, будет первообразным корнем и по модулю $2p^\alpha$.

§ 3. Разыскание первообразных корней по модулям p^α и $2p^\alpha$.

Первообразные корни по модулям p^α и $2p^\alpha$, где p — простое нечётное и $\alpha \geqslant 1$, можно разыскивать, пользуясь следующей общей теоремой:

Пусть $c=\varphi(m)$ и $q_1, q_2, \ldots, q_k$ — различные простые делители числа c. Для того чтобы число g, взаимно простое с m, было первообразным корнем по модулю m, необходимо и достаточно, чтобы это g не удовлетворяло ни одному из сравнений

$$g^{\frac{c}{q_1}} \equiv 1 \pmod m,\ g^{\frac{c}{q_2}} \equiv 1 \pmod m,\ \ldots,\ g^{\frac{c}{q_k}} \equiv 1 \pmod m. \quad (1)$$

Действительно, если g — первообразный корень, то тем самым оно принадлежит показателю c и, следовательно, ни одному из сравнений (1) удовлетворять не может.

Обратно, допустим, что g не удовлетворяет ни одному из сравнений (1). Если бы показатель δ, которому принадлежит g, оказался меньше c, то, обозначая буквою q один из простых делителей $\frac{c}{\delta}$, мы имели бы $\frac{c}{\delta}=qu$, $\frac{c}{q}=\delta u$, $g^{\frac{c}{q}} \equiv 1 \pmod p$, что противоречит нашему допущению. Значит, $\delta=c$ и g — первообразный корень.

Пример 1. Пусть $m=41$. Имеем $\varphi(41)=40=2^3\cdot 5$, $\frac{40}{2}=8$, $\frac{40}{5}=20$. Следовательно, для того чтобы число g, не делящееся на 41, было первообразным корнем по

модулю 41, необходимо и достаточно, чтобы это g не удовлетворяло ни одному из сравнений

$$g^8 \equiv 1 \pmod{41}, \quad g^{20} \equiv 1 \pmod{41}. \tag{2}$$

Но, испытывая числа 2, 3, 4, ..., находим (по модулю 41)

$$2^8 \equiv 10, \quad 3^8 \equiv 1, \quad 4^8 \equiv 18, \quad 5^8 \equiv 18, \quad 6^8 \equiv 10,$$

$$2^{20} \equiv 1, \quad 4^{20} \equiv 1, \quad 5^{20} \equiv 1, \quad 6^{20} \equiv 40.$$

Отсюда видим, что числа 2, 3, 4, 5 — не первообразные корни, так как каждое из них удовлетворяет, по крайней мере, одному из сравнений (2). Число 6 — первообразный корень, так как оно не удовлетворяет ни одному из сравнений (2).

Пример 2. Пусть $m = 1681 = 41^2$. Первообразный корень и здесь можно было бы найти, пользуясь общей теоремой. Но мы найдём его проще, применяя теорему **e**, § 2. Зная уже (пример 1), что первообразный корень по модулю 41 есть 6, находим

$$6^{40} = 1 + 41\,(3 + 41l),$$

$$(6 + 41l)^{40} = 1 + 41\,(3 + 41l - 6^{39}t + 41T) = 1 + 41u.$$

Чтобы u не делилось на 41 достаточно взять $t = 0$. Поэтому в качестве первообразного корня по модулю 1681 можно взять число $6 + 41 \cdot 0 = 6$.

Пример 3. Пусть $m = 3362 = 2 \cdot 1681$. Первообразный корень и здесь можно было бы найти, пользуясь общей теоремой. Но мы найдём его проще, применяя теорему **f**, § 2. Зная уже (пример 2), что первообразный корень по модулю 1681 есть 6, в качестве первообразного корня по модулю 3362 можно взять нечётное из чисел 6, $6 + 1681$, т. е. число 1687.

§ 4. Индексы по модулям p^α и $2p^\alpha$.

a. Пусть p — простое нечётное, $\alpha \geqslant 1$; m — одно из чисел p^α и $2p^\alpha$; $c = \varphi(m)$, g — первообразный корень по модулю m.

b. *Если γ пробегает наименьшие неотрицательные вычеты $\gamma = 0, 1, \ldots, c-1$ по модулю c, то g^γ пробегает приведённую систему вычетов по модулю m.*

Действительно, g^γ пробегает c чисел, взаимно простых с m и, ввиду **b**, § 1, не сравнимых по модулю m.

c. Для чисел a, взаимно простых с m, введём понятие об индексе, представляющее аналогию понятию о логарифме; при этом первообразный корень играет роль, аналогичную роли основания логарифмов.

Если

$$a \equiv g^\gamma \pmod{m}$$

(считаем $\gamma \geqslant 0$), то γ называется *индексом числа a по модулю m при основании g* и обозначается символом $\gamma = \operatorname{ind} a$ (точнее $\gamma = \operatorname{ind}_g a$).

Ввиду **b** всякое a, взаимно простое с m, имеет некоторый единственный индекс γ' среди чисел ряда

$$\gamma = 0, 1, \ldots, c-1.$$

Зная γ', мы можем указать и все индексы числа a; согласно **c**, § 1 это будут все неотрицательные числа класса

$$\gamma \equiv \gamma' \pmod{c}.$$

Непосредственно из данного здесь определения индекса следует, что числа с данным индексом γ образуют класс чисел по модулю m.

d. *Имеем*

$$\operatorname{ind} ab \ldots l \equiv \operatorname{ind} a + \operatorname{ind} b + \ldots + \operatorname{ind} l \pmod{c}$$

и, в частности,

$$\operatorname{ind} a^n \equiv n \operatorname{ind} a \pmod{c}.$$

Действительно,

$$a \equiv g^{\operatorname{ind} a} \pmod{m}, \quad b \equiv g^{\operatorname{ind} b} \pmod{m}, \ldots$$

$$\ldots, \quad l \equiv g^{\operatorname{ind} l} \pmod{m},$$

откуда, перемножая, находим

$$ab \ldots l \equiv g^{\operatorname{ind} a + \operatorname{ind} b + \ldots + \operatorname{ind} l} \pmod{m}.$$

Следовательно, $\operatorname{ind} a + \operatorname{ind} b + \ldots + \operatorname{ind} l$ — один из индексов произведения $ab \ldots l$.

c. Ввиду практической пользы индексов для каждого простого модуля p (разумеется, не слишком большого) составлены *таблицы индексов*. Это две таблицы; одна — для нахождения индекса по числу, другая — для нахождения числа по индексу. Таблицы содержат наименьшие неотрицательные вычеты чисел (приведённая система) и их наименьших индексов (полная система) соответственно по модулям p и $c = \varphi(p) = p - 1$.

Пример. Построим указанные таблицы для модуля $p = 41$. Выше было показано (пример 1, § 3), что первообразным корнем по модулю 41 будет $g = 6$; его мы примем за основание индексов. Находим (сравнения берутся по модулю 41):

$6^0 \equiv 1$	$6^8 \equiv 10$	$6^{16} \equiv 18$	$6^{24} \equiv 16$	$6^{32} \equiv 37$
$6^1 \equiv 6$	$6^9 \equiv 19$	$6^{17} \equiv 26$	$6^{25} \equiv 14$	$6^{33} \equiv 17$
$6^2 \equiv 36$	$6^{10} \equiv 32$	$6^{18} \equiv 33$	$6^{26} \equiv 2$	$6^{34} \equiv 20$
$6^3 \equiv 11$	$6^{11} \equiv 28$	$6^{19} \equiv 34$	$6^{27} \equiv 12$	$6^{35} \equiv 38$
$6^4 \equiv 25$	$6^{12} \equiv 4$	$6^{20} \equiv 40$	$6^{28} \equiv 31$	$6^{36} \equiv 23$
$6^5 \equiv 27$	$6^{13} \equiv 24$	$6^{21} \equiv 35$	$6^{29} \equiv 22$	$6^{37} \equiv 15$
$6^6 \equiv 39$	$6^{14} \equiv 21$	$6^{22} \equiv 5$	$6^{30} \equiv 9$	$6^{38} \equiv 8$
$6^7 \equiv 29$	$6^{15} \equiv 3$	$6^{23} \equiv 30$	$6^{31} \equiv 13$	$6^{39} \equiv 7$

поэтому указанные таблицы будут

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

Здесь номер строки указывает число десятков, номер столбца — число единиц числа (индекса). В графе, общей указанным строке и столбцу, помещается соответствующий индекс (число).

Например, $\operatorname{ind} 25$ найдём в графе первой таблицы, общей строке с номером 2 и столбцу с номером 5, т. е. $\operatorname{ind} 25 = 4$. Число, индекс которого 33, найдём в графе второй таблицы, общей строке с номером 3 и столбцу с номером 3, т. е. $33 = \operatorname{ind} 17$.

§ 5. Следствия предыдущей теории.

a. Пусть p — простое нечётное: $\alpha \geqslant 1$, m — одно из чисел p^α, $2p^\alpha$, наконец, $c = \varphi(m)$.

b. *Пусть* $(n, c) = d$; *тогда*:

1. *Сравнение*

$$x^n \equiv a \pmod m \tag{1}$$

разрешимо (*и тем самым* a *есть вычет степени* n *по модулю* m) *тогда и только тогда, когда* $\operatorname{ind} a$ *кратен* d.

В случае разрешимости сравнение имеет d *решений.*

2. *В приведённой системе вычетов по модулю* m *число вычетов степени* n *есть* $\frac{c}{d}$.

Действительно, сравнение (1) равносильно такому:

$$n \operatorname{ind} x \equiv \operatorname{ind} a \pmod c, \tag{2}$$

которое разрешимо тогда и только тогда, когда $\operatorname{ind} a$ кратен d (d, § 2, гл. IV).

В случае разрешимости сравнения (2) найдём d несравнимых по модулю c значений для $\operatorname{ind} x$; им отвечает d несравнимых по модулю m значений для x.

Таким образом верно утверждение **1.**

Среди чисел $0, 1, \ldots, c-1$, являющихся наименьшими индексами вычетов приведённой системы по модулю m, имеется $\frac{c}{d}$ кратных d. Поэтому верно утверждение **2.**

Пример 1. Для сравнения

$$x^8 \equiv 23 \pmod{41} \tag{3}$$

имеем $(8, 40) = 8$, причём $\operatorname{ind} 23 = 36$ не делится на 8. Поэтому сравнение (3) неразрешимо.

Пример 2. Для сравнения

$$x^{12} \equiv 37 \pmod{41} \qquad (4)$$

имеем $(12, 40) = 4$, причём $\operatorname{ind} 37 = 32$ делится на 4. Поэтому сравнение (4) разрешимо, причём это сравнение имеет 4 решения. Указанные решения найдём следующим образом.

Сравнение (4) равносильно таким:

$$12 \operatorname{ind} x \equiv 32 \pmod{40}, \quad \operatorname{ind} x \equiv 6 \pmod{10}.$$

Отсюда для $\operatorname{ind} x$ найдём 4 несравнимых по модулю 40 значения:

$$\operatorname{ind} x = 6,\ 16,\ 26,\ 36,$$

соответственно чему найдём 4 решения сравнения (4)

$$x \equiv 39;\ 18;\ 2;\ 23 \pmod{41}.$$

Пример 3. Числа

$$1,\ 4,\ 10,\ 16,\ 18,\ 23,\ 25,\ 31,\ 37,\ 40, \qquad (5)$$

индексы которых кратны 4, суть все биквадратичные вычеты (или также вычеты любой степени $n = 12, 28, 36, \ldots$, где $(n, 40) = 4$), имеющиеся среди наименьших положительных вычетов по модулю 41. Число чисел ряда (5) есть $10 = \frac{40}{4}$;

c. Одновременно с утверждением **b, 1** полезно следующее:

Число a есть вычет степени n по модулю m тогда и только тогда, когда

$$a^{\frac{c}{d}} \equiv 1 \pmod{m}. \qquad (6)$$

Действительно, условие $\operatorname{ind} a \equiv 0 \pmod{d}$ равносильно такому: $\frac{c}{d} \operatorname{ind} a \equiv 0 \pmod{c}$. Последнее же равносильно условию (6).

Пример. В теореме § 3 невозможность сравнения $g^{\frac{c}{q}} \equiv 1 \pmod{m}$ равносильна условию, что g — невычет

степени q по модулю m. В частности, невозможность сравнения $g^{\frac{c}{2}} \equiv 1 \pmod{m}$ равносильна условию, что g — квадратичный невычет по модулю m (ср. **e**, § 1, гл. V).

d. 1. *Показатель δ, которому a принадлежит по модулю m, определяется равенством* $(\operatorname{ind} a, c) = \frac{c}{\delta}$; *в частности, принадлежность a к числу первообразных корней по модулю m определяется равенством* $(\operatorname{ind} a, c) = 1$.

2. *В приведённой системе вычетов по модулю m число чисел, принадлежащих показателю δ, есть $\varphi(\delta)$; в частности, число первообразных корней есть $\varphi(c)$.*

Действительно, δ есть наименьший делитель c с условием $a^{\delta} \equiv 1 \pmod{m}$. Это условие равносильно

$$\delta \operatorname{ind} a \equiv 0 \pmod{c},$$

или

$$\operatorname{ind} a \equiv 0 \left(\bmod \frac{c}{\delta}\right).$$

Значит, δ — наименьший делитель c, при котором $\frac{c}{\delta}$ делит $\operatorname{ind} a$, отсюда $\frac{c}{\delta}$ — наибольший делитель c, делящий $\operatorname{ind} a$, т. е. $\frac{c}{\delta} = (\operatorname{ind} a, c)$. Поэтому верно утверждение **1.**

Среди чисел $0, 1, \ldots, c-1$, являющихся наименьшими индексами вычетов приведённой системы по модулю m, кратными $\frac{c}{\delta}$ являются числа вида $\frac{c}{\delta} y$, где $y = 0, 1, \ldots, \delta - 1$. Условие $\left(\frac{c}{\delta} y, c\right) = \frac{c}{\delta}$ равносильно условию $(y, \delta) = 1$; последнему удовлетворяет $\varphi(\delta)$ значений y. Поэтому верно утверждение **2.**

Пример 1. В приведённой системе вычетов по модулю 41 числами, принадлежащими показателю 10, являются числа a с условием $(\operatorname{ind} a, 40) = \frac{40}{10} = 4$, т. е. числа

$$4,\ 23,\ 25,\ 31.$$

Число этих чисел есть $4 = \varphi(10)$.

Пример 2. В приведённой системе вычетов по модулю 41 первообразными корнями являются числа a с условием $(\mathrm{ind}\, a, 40) = 1$, т. е. числа
6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35.
Число этих первообразных корней есть $16 = \varphi(40)$.

§ 6. Индексы по модулю 2^α.

a. Для модуля 2^α предыдущая теория заменяется несколько более сложной.

b. Пусть $\alpha = 1$. Тогда $2^\alpha = 2$. Имеем $\varphi(2) = 1$. Первообразным корнем по модулю 2 будет, например, $1 \equiv -1 \pmod 2$. Число $1^0 = (-1)^0 = 1$ образует приведённую систему вычетов по модулю 2.

c. Пусть $\alpha = 2$. Тогда $2^\alpha = 4$. Имеем $\varphi(4) = 2$. Первообразным корнем по модулю 4 будет, например, $3 \equiv -1 \pmod 4$. Числа $(-1)^0 = 1$, $(-1)^1 \equiv 3 \pmod 4$ образуют приведённую систему вычетов по модулю 4.

d. Пусть $\alpha \geqslant 3$. Тогда $2^\alpha \geqslant 8$. Имеем $\varphi(2^\alpha) = 2^{\alpha-1}$. Нетрудно видеть, что первообразных корней в этом случае нет; более точно: показатель, которому принадлежит по модулю 2^α нечётное число x, не превосходит $2^{\alpha-2} = \frac{1}{2}\varphi(2^\alpha)$. Действительно, имеем

$$x^2 = 1 + 8t_1,$$
$$x^4 = 1 + 16t_2,$$
$$\cdots\cdots\cdots$$
$$x^{2^{\alpha-2}} = 1 + 2^\alpha t_{\alpha-2} \equiv 1 \pmod{2^\alpha}.$$

При этом числа, принадлежащие показателю $2^{\alpha-2}$, существуют. Таким числом будет, например, 5. Действительно,

$$5 = 1 + 4,$$
$$5^2 = 1 + 8 + 16,$$
$$5^4 = 1 + 16 + 32u_2,$$
$$\cdots\cdots\cdots\cdots$$
$$5^{2^{\alpha-3}} = 1 + 2^{\alpha-1} + 2^\alpha u_{\alpha-3},$$

откуда видим, что ни одна из степеней $5^1, 5^2, 5^4, \ldots, 5^{2^{\alpha-3}}$ не сравнима с 1 по модулю 2^α.

Нетрудно видеть, что числа двух следующих строк:

$$5^0, \quad 5^1, \ldots, \quad 5^{2^{\alpha-2}-1},$$
$$-5^0, -5^1, \ldots, -5^{2^{\alpha-2}-1}$$

образуют приведённую систему вычетов по модулю 2^α. Действительно, число этих чисел будет $2 \cdot 2^{\alpha-2} = \varphi(2^\alpha)$; числа каждой отдельно взятой строки между собой по модулю 2^α несравнимы (b, § 1); наконец, числа верхней строки несравнимы с числами нижней, так как первые по модулю 4 сравнимы с 1, а вторые с -1.

e. Для удобства дальнейших исследований мы выразим результаты b, c, d в более единообразной форме, которая будет пригодна и в случае $\alpha = 0$.

Пусть

$$c = 1; \quad c_0 = 1, \qquad \text{если } \alpha = 0, \text{ или } \alpha = 1;$$
$$c = 2, \quad c_0 = 2^{\alpha-2}, \quad \text{если } \alpha \geqslant 2$$

(таким образом всегда $cc_0 = \varphi(2^\alpha)$) и пусть γ и γ_0 независимо друг от друга пробегают наименьшие неотрицательные вычеты

$$\gamma = 0, \ldots, c-1; \quad \gamma_0 = 0, \ldots, c_0 - 1$$

по модулям c и c_0. Тогда $(-1)^\gamma 5^{\gamma_0}$ пробегает приведённую систему вычетов по модулю 2^α.

f. *Сравнение*

$$(-1)^\gamma 5^{\gamma_0} \equiv (-1)^{\gamma'} 5^{\gamma_0'} \pmod{2^\alpha} \tag{1}$$

имеет место тогда и только тогда, когда

$$\gamma \equiv \gamma' \pmod c, \quad \gamma_0 \equiv \gamma_0' \pmod{c_0}.$$

Действительно, при $\alpha = 0$ теорема очевидна. Поэтому предположим, что $\alpha > 0$. Пусть наименьшие неотрицательные вычеты по модулям c и c_0 для чисел γ и γ_0 будут r и r_0, а для чисел γ' и γ_0' будут r' и r_0'. Ввиду c, § 1 (-1 принадлежит показателю c, а 5 принадлежит показателю c_0), сравнение (1) имеет место тогда

и только тогда, когда $(-1)^{r}5^{r_0} \equiv (-1)^{r'}5^{r'_0} \pmod{2^\alpha}$, т. е. (ввиду e) когда $r = r'$, $r_0 = r'_0$.

g. Если

$$a \equiv (-1)^{\gamma}5^{\gamma_0} \pmod{2^\alpha},$$

то система γ, γ_0 называется *системой индексов числа a по модулю 2^α*.

Ввиду e всякое a, взаимно простое с 2^α (т. е. нечётное), имеет единственную систему индексов γ', γ'_0 среди $cc_0 = \varphi(2^\alpha)$ пар значений γ, γ_0, указанных в e.

Зная систему $\gamma'\gamma'_0$, мы можем указать и все системы индексов числа a; согласно f это будут все пары γ, γ_0, составленные из неотрицательных чисел классов

$$\gamma \equiv \gamma' \pmod{c}, \quad \gamma_0 \equiv \gamma'_0 \pmod{c_0}.$$

Непосредственно из данного здесь определения системы индексов следует, что числа с данной системой индексов γ, γ_0 образуют класс чисел по модулю 2^α.

h. *Индексы произведения сравнимы по модулям c и c_0 с суммами индексов сомножителей.*

Действительно, пусть $\gamma(a)$, $\gamma_0(a)$; ...; $\gamma(l)$, $\gamma_0(l)$ — системы индексов чисел a, ..., l. Имеем

$$a \dots l \equiv (-1)^{\gamma(a)+\dots+\gamma(l)}5^{\gamma_0(a)+\dots+\gamma_0(l)}.$$

Следовательно, $\gamma(a) + \dots + \gamma(l)$, $\gamma_0(a) + \dots + \gamma_0(l)$ — индексы произведения $a \dots l$.

§ 7. Индексы по любому составному модулю.

a. Пусть $m = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ — каноническое разложение числа m. Пусть далее c и c_0 имеют значения, указанные в e, § 6; $c_s = \varphi(p_s^{\alpha_s})$; g_s — наименьший первообразный корень по модулю $p_s^{\alpha_s}$.

b. Если

$$\left.\begin{aligned} a &\equiv (-1)^{\gamma}5^{\gamma_0} \pmod{2^\alpha}, \\ a &\equiv g_1^{\gamma_1} \pmod{p_1^{\alpha_1}}, \dots, a \equiv g_k^{\gamma_k} \pmod{p_k^{\alpha_k}}; \end{aligned}\right\} \quad (1)$$

то система γ, γ_0, γ_1, ..., γ_k называется *системой индексов числа a по модулю m*.

Из такого определения следует, что γ, γ_0 — система индексов числа a по модулю 2^α, а γ_1, ..., γ_k — индексы числа a по модулям $p_1^{\alpha_1}$, ..., $p_k^{\alpha_k}$. Поэтому (g, § 6; c, § 4) всякое a, взаимно простое с m (тем самым оно взаимно простое и со всеми 2^α, $p_1^{\alpha_1}$, ..., $p_k^{\alpha_k}$), имеет единственную систему индексов γ', γ'_0, γ'_1, ..., γ'_k среди $cc_0c_1 \dots c_k = \varphi(m)$ систем γ, γ_0, γ_1, ..., γ_k, которые получим, заставляя γ, γ_0, γ_1, ..., γ_k независимо друг от друга пробегать наименьшие неотрицательные вычеты по модулям c, c_0, c_1, ..., c_k, а все системы индексов числа a суть все системы γ, γ_0, γ_1, ..., γ_k, составленные из неотрицательных чисел классов

$$\gamma \equiv \gamma' \pmod{c}, \quad \gamma_0 \equiv \gamma'_0 \pmod{c_0},$$

$$\gamma_1 \equiv \gamma'_1 \pmod{c_1}, \dots, \gamma_k \equiv \gamma'_k \pmod{c_k}.$$

Числа a с данной системой индексов γ, γ_0, γ_1, ..., γ_k могут быть найдены путём решения системы (1), а следовательно (b, § 3, гл. IV), образуют класс чисел по модулю m.

c. Так как индексы γ, γ_0, γ_1, ..., γ_k числа a по модулю m являются индексами его соответственно по модулям 2^α, $p_1^{\alpha_1}$, ..., $p_k^{\alpha_k}$, то верна теорема:

Индексы произведения сравнимы по модулям c, c_0, c_1, ..., c_k с суммами индексов сомножителей.

d. Пусть $\tau = \varphi(2^\alpha)$ при $\alpha \leqslant 2$ и $\tau = \frac{1}{2}\varphi(2^\alpha)$ при $\alpha > 2$ и пусть h — общее наименьшее кратное чисел τ, c_1, ..., c_k. При всяком a, взаимно простом с m, сравнение $a^h \equiv 1$ верно по всем модулям 2^α, $p_1^{\alpha_1}$, ..., $p_k^{\alpha_k}$, значит, это сравнение верно и по модулю m. Поэтому a не может быть первообразным корнем по модулю m в тех случаях, когда $h < \varphi(m)$. Но последнее имеет место при $\alpha > 2$, при $k > 1$, а также при $\alpha = 2$, $k = 1$. Поэтому для $m > 1$ первообразные корни могут существовать лишь в случаях $m = 2, 4, p_1^{\alpha_1}, 2p_1^{\alpha_1}$. Но как раз для

этих случаев существование первообразных корней было доказано выше (§ 6, § 2). Поэтому

Все случаи, когда существуют первообразные корни по модулю m, превосходящему 1, суть

$$m = 2,\ 4,\ p^\alpha,\ 2p^\alpha.$$

Вопросы к главе VI.

Буквою p здесь всегда обозначаем простое нечётное число, а в вопросе 11, b также и число 2.

1. a. Пусть a — целое, $a > 1$. Доказать, что простые нечётные делители числа $a^n - 1$ делят $a - 1$ или имеют вид $2px + 1$.

b. Пусть a — целое, $a > 1$. Доказать, что простые нечётные делители числа $a^n + 1$ делят $a + 1$ или имеют вид $2px + 1$.

c. Доказать бесконечность числа простых чисел вида $2px + 1$.

d. Пусть n — целое, $n > 0$. Доказать, что простые делители числа $2^{2^n} + 1$ имеют вид $2^{n+1}x + 1$.

2. Пусть a — целое, $a > 1$, n — целое, $n > 0$. Доказать, что $\varphi(a^n - 1)$ кратно n.

3, a. Пусть n — целое, $n > 1$. Из чисел 1, 2, ..., n при нечётном n образуем перестановки

$$1,\ 3,\ 5,\ \ldots,\ n-2,\ n,\ n-1,\ n-3,\ \ldots,\ 4,\ 2;$$

$$1,\ 5,\ 9,\ \ldots,\ 7,\ 3$$

и т. д., а при чётном n образуем перестановки

$$1,\ 3,\ 5,\ \ldots,\ n-1,\ n,\ n-2,\ \ldots,\ 4,\ 2;$$

$$1,\ 5,\ 9,\ \ldots,\ 7,\ 3,$$

и т. д. Доказать, что k-я операция даёт исходный ряд тогда и только тогда, когда $2^k \equiv \pm 1 \pmod{2n-1}$.

b. Пусть n — целое, $n > 1$, m — целое, $m > 1$. Будем считать числа 1, 2, ..., n в прямом порядке от 1 до n, далее в обратном порядке от n до 2, затем опять в прямом порядке от 1 до n, далее опять в обратном порядке от n до 2 и т. д. При таком счёте выписываем числа 1-е, $(m+1)$-е, $(2m+1)$-е и т. д., пока не получим n чисел. С этим новым рядом n чисел повторим ту же операцию и т. д. Доказать, что k-я операция даёт исходный ряд тогда и только тогда, когда

$$m^k \equiv \pm 1 \pmod{2n-1}.$$

4. Существование $\varphi(d)$ чисел, принадлежащих показателю d, доказать, рассматривая сравнение $x^d \equiv 1 \pmod p$ (вопрос 10 c, гл. IV) и применяя **d**, § 3, гл. II.

5, a. Доказать, что первообразный корень простого числа вида $2^n + 1$, $n > 1$ есть 3.

b. Доказать, что первообразный корень простого числа вида $2p + 1$ при p вида $4n - 1$ есть 2, а при p вида $4n + 3$ есть -2.

c. Доказать, что первообразный корень простого числа вида $4p + 1$ есть 2.

d. Доказать, что первообразный корень простого числа вида

$$2^n p + 1 \text{ при } n > 1 \text{ и } p > \frac{3^{2^{n-1}}}{2^n} \text{ есть } 3.$$

6, a α) Пусть n — целое, $n > 0$, $S = 1^n + 2^n + \ldots + (p-1)^n$. Доказать, что

$$S \equiv -1 \pmod p, \quad \text{если } n \text{ кратно } p-1,$$

$$S \equiv 0 \pmod p \quad \text{в противном случае.}$$

β) При обозначениях вопроса 9, c, гл. V доказать, что

$$S(1) \equiv -\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \pmod p.$$

b. Теорему Вильсона доказать, применяя **b**, § 4.

7. Пусть g и g_1 — первообразные корни по модулю p, а $\operatorname{ind}_g g_1 \equiv 1 \pmod{p-1}$.

a. Пусть $(a, p) = 1$. Доказать, что

$$\operatorname{ind}_{g_1} a \equiv \operatorname{ind}_g a \pmod{p-1}.$$

b. Пусть n — делитель $p-1$, $1 < n < p-1$. Числа, взаимно простые с p, можно разбить на n совокупностей, отнеся к s-й совокупности ($s = 0, 1, \ldots, n-1$) числа с условием $\operatorname{ind} a \equiv s \pmod n$. Доказать, что совокупность, имеющая при основании g номер s, тождественна совокупности, имеющей при основании g_1 номер s_1, где $s_1 \equiv as \pmod n$.

8. Указать возможно более простой способ решения сравнения $x^n \equiv a \pmod p$ (удобный, если $(n, p-1)$ невелико) в случае, когда известен некоторый первообразный корень g по модулю p.

9. Пусть m, a, c, c_0, c_1, ..., c_k, γ, γ_0, γ_1, ..., γ_k имеют значения, указанные в § 7. Взяв какие-либо корни R, R_0, R_1, ..., R_k уравнений

$$R^c = 1,\ R_0^{c_0} = 1,\ R_1^{c_1} = 1,\ \ldots,\ R_k^{c_k} = 1,$$

полагаем

$$\chi(a) = R^\gamma R_0^{\gamma_0} R_1^{\gamma_1} \ldots R_k^{\gamma_k}.$$

Если $(a, m) > 1$, то полагаем $\chi(a) = 0$.

Определённую таким образом для всех целых a функцию назовем *характером*. При $R=R_0=R_1=\ldots=R_k=1$ характер назовём *главным*; он имеет значение 1 при $(a, m)=1$ и значение 0 при $(a, m)>1$.

a. Доказать, что указанным путём мы получим $\varphi(m)$ различных характеров (два характера называются различными, если они, по крайней мере, при одном значении a не равны между собою).

b. Вывести следующие свойства характеров:

α) $\chi(1)=1$,

β) $\chi(a_1a_2)=\chi(a_1)\,\chi(a_2)$,

γ) $\chi(a_1)=\chi(a_2)$, если $a_1\equiv a_2 \pmod m$.

c. Доказать, что

$$\sum_{a=0}^{m-1}\chi(a)=\begin{cases}\varphi(m) & \text{для главного характера,}\\ 0 & \text{для других характеров.}\end{cases}$$

d. Доказать, что, суммируя при данном a по всем $\varphi(m)$ характерам, имеем

$$\sum_{\chi}\chi(a)=\begin{cases}\varphi(m), & \text{если } a\equiv 1 \pmod m,\\ 0 & \text{в противном случае}\end{cases}$$

e. Рассматривая сумму

$$H=\sum_{\chi}\sum_{a}\frac{\chi(a)}{\psi(a)},$$

где a пробегает приведённую систему вычетов по модулю m, доказать, что функция $\psi(a)$, определённая для всех целых a, удовлетворяющая условиям

$\psi(a)=0$, если $(a, m)>1$,

$\psi(a)$ не равна тождественно 0,

$\psi(a_1a_2)=\psi(a_1)\,\psi(a_2)$,

$\psi(a_1)=\psi(a_2)$, если $a_1\equiv a_2 \pmod m$,

есть характер.

f. Доказать следующие теоремы.

α) Если $\chi_1(a)$ и $\chi_2(a)$—характеры, то $\chi_1(a)\,\chi_2(a)$—также характер.

β) Если $\chi_1(a)$—характер и $\chi(a)$ пробегает все характеры, то $\chi_1(a)\,\chi(a)$ также пробегает все характеры.

γ) При $(l, m)=1$ имеем

$$\sum_{\chi}\frac{\chi(a)}{\chi(l)}=\begin{cases}\varphi(m), & \text{если } a\equiv l \pmod m,\\ 0 & \text{в противном случае}\end{cases}$$

10, a. Пусть n—делитель $p-1$, $1<n\leqslant p-1$, l—целое, не делящееся на n. Число $R_1=e^{2\pi i\frac{l}{n}}$ является корнем уравнения $R_1^n=1$ и, следовательно, степень $e^{2\pi i\frac{l\operatorname{ind}x}{n}}$, которой при x, кратном p, следует приписывать значение 0, есть характер по модулю p.

α) При $(k, p)=1$ доказать, что

$$\sum_{x=1}^{p-1}e^{2\pi i\frac{l\operatorname{ind}(x+k)-l\operatorname{ind}x}{n}}=-1.$$

β) Пусть Q—целое, $1<Q<p$,

$$S=\sum_{x\ 0}^{p-1}|S_{l,\,n,\,x}|^2;\quad S_{l,\,n,\,x}=\sum_{z=0}^{Q-1}e^{2\pi i\frac{l\operatorname{ind}(x+z)}{n}}$$

Доказать, что $S=(p-Q)Q$.

γ) Пусть $p>4n^2$, $n>2$, M—целое. Доказать, что в ряде $M, M+1, \ldots, M+2[n\sqrt{p}]-1$ имеется число s-й совокупности вопроса 7, b.

b. Пусть $p>4\left(\frac{p-1}{\varphi(p-1)}\right)^2 2^{2k}$, k—число различных простых делителей $p-1$, M—целое. Доказать, что в ряде $M, M+1, \ldots, M+2\left[\frac{p-1}{\varphi(p-1)}2^k\sqrt{p}\right]-1$ имеется первообразный корень по модулю p.

11, a. Пусть a—целое, n—делитель $p-1$, $1<n\leqslant p-1$, k—целое, не делящееся на n,

$$U_{a,\,p}=\sum_{x=1}^{p-1}e^{2\pi i\frac{k\operatorname{ind}x}{n}}\,e^{2\pi i\frac{ax}{p}}.$$

α) При $(a, p)=1$ доказать, что $|U_{a,\,p}|=\sqrt{p}$.

β) Доказать, что

$$e^{2\pi i\frac{-k\operatorname{ind}a}{n}}=\frac{U_{a,\,p}}{U_{1,\,p}}$$

γ) Пусть p имеет вид $4m+1$,

$$S=\sum_{x=1}^{p-2} e^{2\pi i\frac{\operatorname{ind}(x^2+x)}{4}}.$$

Доказать, что (ср. вопросы 9, a и 9, c, гл. V) $p=A^2+B^2$, где A и B — целые, определяемые равенством $S=A+Bi$.

b. Пусть n — целое, $n>2$, $m>1$, $(a, m)=1$,

$$S_{a,m}=\sum_{x} e^{2\pi i\frac{ax^n}{m}},\quad S'_{a,m}=\sum_{\xi}{}' e^{2\pi i\frac{a\xi^n}{m}},$$

где x пробегает полную, а ξ — приведённую системы вычетов по модулю m (ср. вопрос 12, d, гл. III и вопрос 11, b, гл. V)

α) Пусть $\delta=(n, p-1)$. Доказать, что

$$|S_{a,p}|\leqslant(\delta-1)\sqrt{p}.$$

β) Пусть $(n, p)=1$, s — целое, $1<s\leqslant n$. Доказать, что

$$S_{a,p^s}=p^{s-1},\quad S'_{a,p^s}=0.$$

γ) Пусть s — целое, $s>n$. Доказать, что

$$S_{a,p^s}=p^{n-1}S_{a,p^{s-n}},\quad S'_{a,p^s}=0.$$

δ) Доказать, что

$$|S_{a,m}|<Cm^{1-\frac{1}{n}},$$

где C зависит только от n.

12. Пусть M и Q — целые, $0<M<M+Q\leqslant p$.

a. Пусть n — делитель $p-1$, $1<n<p-1$, k — целое, не делящееся на n. Доказать, что

$$\left|\sum_{x=M}^{M+Q-1} e^{2\pi i\frac{k\operatorname{ind}x}{n}}\right|<\sqrt{p}\ln p.$$

b. Пусть T — число чисел s-й совокупности вопроса 7, b, заключённых среди чисел M, $M+1$, ..., $M+Q-1$. Доказать, что

$$T=\frac{Q}{n}+\vartheta\sqrt{p}\ln p;\quad|\vartheta|<1.$$

c. Пусть k — число простых делителей $p-1$, H — число первообразных корней по модулю p, заключённых среди чисел M, $M+1$, ..., $M+Q-1$. Доказать, что

$$H=\frac{\varphi(p-1)}{p-1}Q+\vartheta 2^k\sqrt{p}\ln p;\quad|\vartheta|<1$$

d. Пусть M_1 и Q_1 — целые, $0\leqslant M_1<M_1+Q_1\leqslant p-1$, J — число чисел ряда $\operatorname{ind}M$, $\operatorname{ind}(M+1)$, ..., $\operatorname{ind}(M+Q-1)$, заключённых среди чисел ряда M_1, M_1+1, ..., M_1+Q_1-1. Доказать, что

$$J=\frac{QQ_1}{p-1}+\vartheta\sqrt{p}(\ln p)^2;\quad|\vartheta|<1.$$

13. Доказать существование постоянного p_0 с условием: если $p>p_0$, n — делитель $p-1$, $1<n<p-1$, то наименьший из положительных невычетов степени n по модулю p будет

$$<h;\quad h=p^{\frac{1}{c}}(\ln p)^2;\quad c=2e^{1-\frac{1}{n}}.$$

14. a. Пусть $m>1$, $(a, m)=1$,

$$S=\sum_{x=0}^{m-1}\sum_{y=0}^{m-1}\nu(x)\mu(y)e^{2\pi i\frac{axy}{m}};\quad\sum_{x=0}^{m-1}|\nu(x)|^2=X,$$

$$\sum_{y=0}^{m-1}|\mu(y)|^2=Y.$$

Доказать, что $|S|\leqslant\sqrt{XYm}$.

b, α) Пусть $m>1$, $(a, m)=1$, n — целое, $n>0$, K — число решений сравнения $x^n\equiv1\pmod m$,

$$S=\sum_{x=1}^{m-1}\chi(x)e^{2\pi i\frac{ax^n}{m}}.$$

Доказать, что $|S|\leqslant K\sqrt{m}$.

β) Пусть ε — произвольное положительное постоянное. При постоянном n для числа K вопроса α) доказать, что $K=O(m^\varepsilon)$.

15. a. Пусть $(a, p)=(b, p)=1$, n — целое, $|n|=n_1$, $0<n_1<p$,

$$S=\sum_{x=1}^{p-1} e^{2\pi i\frac{ax^n+bx}{p}}.$$

Доказать, что

$$|S|<\frac{3}{2}n^{\frac{1}{2}}p^{\frac{3}{4}}.$$

b. Пусть $(A, p)=1$, n—целое, $|n|=n_1$, $0<n_1<p$, M_0 и Q_0—целые, $0<M_0<M_0+Q_0\leqslant p$.

α) Пусть

$$S=\sum_{x=M_0}^{M_0+Q_0-1} e^{2\pi i\frac{Ax^n}{p}}.$$

Доказать, что $|S|<\frac{3}{2}n_1^{\frac{1}{2}}p^{\frac{3}{4}}\ln p$.

β) Пусть M и Q—целые, $0<M<M+Q\leqslant p$, T—число чисел ряда Ax^n; $x=M_0$, M_0+1, ..., M_0+Q_0-1, сравнимых по модулю p с числами ряда M, $M+1$, ..., $M+Q-1$.

Доказать, что

$$T=\frac{Q_0Q}{p}+\vartheta\frac{3}{2}n_1^{\frac{1}{2}}p^{\frac{3}{4}}(\ln p)^2;\quad|\vartheta|<1$$

c. Пусть $(a, p)=1$, b и c—целые, $(b^2-4ac, p)=1$.

α) Пусть γ—целое,

$$S=\sum_{x=0}^{p-1}\left(\frac{ax^2+bx+c}{p}\right)e^{2\pi i\frac{\gamma x}{p}}$$

Доказать, что $|S|<\frac{3}{2}p^{\frac{3}{4}}$.

β) Пусть M и Q—целые, $0<M<M+Q\leqslant p$,

$$S=\sum_{x=M}^{M+Q-1}\left(\frac{ax^2+bx+c}{p}\right)$$

Доказать, что $|S|<\frac{3}{2}p^{\frac{3}{4}}\ln p$.

Численные примеры к главе VI.

1, a. Найти (путём возможно более простых вычислений) показатель, которому принадлежит 7 по модулю 43.

b. Найти показатель, которому принадлежит 5 по модулю 108.

2, a. Найти первообразные корни по модулям 17, 289, 578.

b. Найти первообразные корни по модулям 23, 529, 1058.

c. Найти наименьший первообразный корень по модулю 242.

3, a. Составить таблицы индексов по модулю 17.

b. Составить таблицы индексов по модулю 23.

4, a. Найти первообразный корень по модулю 71, применяя указание примера c, § 5.

b. Найти первообразный корень по модулю 191.

5, a. Пользуясь таблицей индексов, указать число решений сравнений:

α) $x^{60}\equiv 79\pmod{97}$, β) $x^{55}\equiv 17\pmod{97}$, γ) $x^{15}\equiv 46\pmod{97}$.

b. Указать число решений сравнений

α) $3x^{12}\equiv 31\pmod{41}$, β) $7x^7\equiv 11\pmod{41}$, γ) $5x^{30}\equiv 37\pmod{41}$.

6, a. Пользуясь таблицей индексов, решить сравнения

α) $x^5\equiv 59\pmod{67}$, β) $x^{55}\equiv 17\pmod{67}$, γ) $x^{30}\equiv 14\pmod{67}$.

b. Решить сравнения

α) $23x^5\equiv 15\pmod{73}$, β) $37x^6\equiv 69\pmod{73}$, γ) $44x^{21}\equiv 53\pmod{73}$.

7, a. Пользуясь теоремой c, § 5, определить число решений сравнений

α) $x^3\equiv 2\pmod{37}$, β) $x^{16}\equiv 10\pmod{37}$

b. Определить число решений сравнений

α) $x^5\equiv 3\pmod{71}$, β) $x^{21}\equiv 5\pmod{71}$.

8, a. Применяя способ вопроса 8, решить сравнения (при решении второго сравнения воспользоваться таблицей первообразных корней в конце книги)

α) $x^7\equiv 37\pmod{101}$, β) $x^9\equiv 44\pmod{101}$.

b. Решить сравнение

$$x^3\equiv 23\pmod{109}.$$

9, a. Пользуясь таблицей индексов, среди вычетов приведённой системы по модулю 19 указать: α) квадратичные вычеты, β) кубические вычеты.

b. Среди вычетов приведённой системы по модулю 37 указать: α) вычеты степени 15, β) вычеты степени 8.

10, a. Среди вычетов приведённой системы по модулю 43 указать: α) числа, принадлежащие показателю 6, β) первообразные корни.

b. Среди вычетов приведённой системы по модулю 61 указать: α) числа, принадлежащие показателю 10, β) первообразные корни.

РЕШЕНИЯ ВОПРОСОВ.

Решения к главе I.

1. Остаток от деления $ax+by$ на d, имея вид $ax'+by'$ и будучи меньше d, непременно равен нулю. Поэтому d — делитель всех чисел вида $ax+by$ и, в частности, общий делитель чисел $a\cdot 1+b\cdot 0=a$ и $a\cdot 0+b\cdot 1=b$. С другой стороны, выражение для d показывает, что всякий общий делитель чисел a и b делит d. Поэтому $d=(a, b)$, и верна теорема 1, d, § 2. Теоремы e, § 2 выводятся так: наименьшее положительное число вида $amx+bmy$ есть amx_0+bmy_0; наименьшее положительное число вида $\frac{a}{\delta}x+\frac{b}{\delta}y$ есть $\frac{a}{\delta}x_0+\frac{b}{\delta}y_0$.

Обобщение этих результатов тривиально.

2. Предварительно заметим, что разность двух неравных между собою рациональных дробей $\frac{k}{l}$ и $\frac{m}{n}$ $(l>0,\quad n>0)$ численно $\geqslant\frac{1}{ln}$. Ограничимся предположением $\delta_s<\delta_{s+1}$. Пусть $\frac{a}{b}$ — несократимая дробь, не равная δ_s, с условием $0<b\leqslant Q_s$. Не может быть $\delta_s<\frac{a}{b}<\delta_{s+1}$; в противном случае было бы

$$\frac{a}{b}-\delta_s\geqslant\frac{1}{bQ_s},$$

$$\delta_{s+1}-\frac{a}{b}\geqslant\frac{1}{bQ_{s+1}},$$

$$\delta_{s+1}-\delta_s>\frac{1}{Q_sQ_{s+1}}.$$

Поэтому $\frac{a}{b}<\delta_s$ или же $\delta_{s+1}<\frac{a}{b}$. В обоих случаях δ_s ближе к α, чем $\frac{a}{b}$.

3. При $n\leqslant 6$ теорема очевидна; поэтому предполагаем $n>6$. Имеем

$$\xi=\frac{1+\sqrt{5}}{2}=1{,}618\ldots;\quad \log_{10}\xi=0{,}2\ldots;$$

$$\begin{aligned}
&Q_2\geqslant 1 && =g_1=1\\
&Q_3\geqslant Q_2+1 && \geqslant g_2=2>\xi,\\
&Q_4\geqslant Q_3+Q_2 && \geqslant g_3=g_2+g_1>\xi+1=\xi^2,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&Q_n>Q_{n-1}+Q_{n-2}\geqslant g_{n-1}=g_{n-2}+g_{n-3}>\xi^{n-3}+\xi^{n-4}=\xi^{n-2}.
\end{aligned}$$

Отсюда

$$N>\xi^{n-2};\quad n<\frac{\log_{10}N}{\log_{10}\xi}+2<5k+2;\quad n\leqslant 5k+1.$$

4, a. Для дробей $\frac{0}{1}$ и $\frac{1}{1}$ имеем $0\cdot 1-1\cdot 1=-1$. Вставляя между дробями $\frac{A}{B}$ и $\frac{C}{D}$ с условием $AD-BC=-1$ дробь $\frac{A+C}{B+D}$, имеем $A(B+D)-B(A+C)=(A+C)D-(B+D)C=-1$. Поэтому верно утверждение, отмеченное в конце вопроса. Существование дроби $\frac{k}{l}$ с условиями $\frac{a}{b}<\frac{k}{l}<\frac{c}{d}$, $l<\tau$ невозможно. В противном случае мы имели бы

$$\frac{k}{l}-\frac{a}{b}\geqslant\frac{1}{lb};\quad \frac{c}{d}-\frac{k}{l}\geqslant\frac{1}{ld};\quad \frac{c}{d}-\frac{a}{b}\geqslant\frac{b+d}{lbd}>\frac{1}{bd}.$$

b. Очевидно, достаточно рассматривать случай $0\leqslant\alpha<1$. Пусть $\frac{a}{b}\leqslant\alpha<\frac{c}{d}$, где $\frac{a}{b}$ и $\frac{c}{d}$ — соседние дроби ряда Фарея, отвечающего τ. Возможны два случая:

$$\frac{a}{b}\leqslant\alpha<\frac{a+c}{b+d};\quad \frac{a+c}{b+d}\leqslant\alpha<\frac{c}{d}.$$

Поэтому верно одно из двух неравенств

$$\left|\alpha-\frac{a}{b}\right|<\frac{1}{b(b+d)};\quad \left|\alpha-\frac{c}{d}\right|\leqslant\frac{1}{d(b+d)},$$

откуда ввиду $b+d>\tau$ указанная теорема следует непосредственно.

c. При α иррациональном теорема следует из h, § 4, если принять за $\frac{P}{Q}$ подходящую дробь $\frac{P_{s-1}}{Q_{s-1}}$, где $Q_{s-1}\leqslant\tau<Q_s$.

В случае же рационального $a=\frac{a}{b}$ приведённое рассуждение осуществимо лишь при $b>\tau$. Но при $b\leqslant\tau$ теорема верна, так как тогда за $\frac{P}{Q}$ можно принять самоё дробь $\frac{a}{b}$, полагая при этом $\vartheta=0$.

5, а. Нечётные простые числа при делении на 4 дают остаток 1 или же 3. Произведение чисел вида $4m+1$ имеет вид $4m+1$. Поэтому число $4p_1\dots p_k-1$, где $p_1,\dots,p_k$ — простые вида $4m+3$, наверно имеет простой делитель q вида $4m+3$. При этом q не совпадает ни с одним из чисел $p_1,\dots,p_k$.

b. Простые числа, превосходящие 3, имеют вид $6m+1$ или же $6m+5$. Число $6p_1\dots p_k-1$, где $p_1,\dots,p_k$ — простые вида $6m+5$, наверно имеет простой делитель q вида $6m+5$. При этом q не совпадает ни с одним из чисел $p_1,\dots,p_k$.

6. Пусть $p_1,\dots,p_k$ — какие-либо k простых чисел и N — целое с условиями $2<N$, $(3\ln N)^k<N$. Число чисел a ряда $1,2,\dots,N$, каноническое разложение которых имеет вид $a=p_1^{\alpha_1}\dots p_k^{\alpha_k}$, ввиду $\alpha_s\leqslant\frac{\ln N}{\ln 2}$ будет

$$\leqslant\left(\frac{\ln N}{\ln 2}+1\right)^k<(3\ln N)^k<N$$

Поэтому в ряде $1,2,\dots,N$ найдутся числа, в каноническое разложение которых входит простые, отличные от $p_1,\dots,p_k$.

7. Например, такие последовательности получим при

$$M=2\cdot 3\dots(K+1)t+2;\quad t=1,2,\dots$$

8. Взяв целое x_0 с условием, что при $x\geqslant x_0$, $f(x)>1$ и $f'(x)>0$, положим $f(x_0)=X$. Составными (кратными X) будут все числа $f(x_0+Xt)$; $t=1,2,\dots$

9, а. При наличии (1) одно из чисел x, y, пусть именно x, будет чётным; из

$$\left(\frac{x}{2}\right)^2=\frac{z+y}{2}\,\frac{z-y}{2},$$

где, очевидно, $\left(\frac{z+y}{2},\ \frac{z-y}{2}\right)=1$, убеждаемся в существовании положительных целых u и v с условиями

$$\frac{x}{2}=uv,\quad \frac{z+y}{2}=u^2,\quad \frac{z-y}{2}=v^2.$$

Отсюда следует необходимость условий, указанных в вопросе.

Достаточность этих условий очевидна.

b. Условимся здесь обозначать буквами лишь целые положительные числа. Допустив существование систем x, y, z, с условиями $x^4+y^4=z^2$, $x>0$, $y>0$, $z>0$, $(x,y,z)=1$, выберем из них систему с наименьшим z. Предполагая x чётным, найдём $x^2=2uv$, $y^2=u^2-v^2$, $u>v\geqslant 1$, $(u,v)=1$, где v — чётное (при чётном u было бы $y^2=4N+1$, $u^2=4N_1$, $v^2=4N_2+1$, $4N+1=4N_1-4N_2-1$, что невозможно). Отсюда $u=z_1^2$, $v=2v_1^2$, $y^2+4v_1^4=z_1^4$, $2v_1^2=2u_1v_1$, $u_1=x_1^2$, $v_1=y_1^2$, $x_1^4-y_1^4=z_1^2$, что ввиду $z_1<z$ невозможно.

Из неразрешимости уравнения $x^4+y^4=z^2$ как частный случай, очевидно, следует и неразрешимость уравнения $x^4+y^4=t^4$ в целых положительных x, y, t.

10. Полагая $x=\frac{k}{l}$; $(k,l)=1$, находим

$$k^n+a_1k^{n-1}l+\dots+a_nl^n=0.$$

Поэтому k^n кратно l и, следовательно, $l=1$.

11, а. Пусть k — наибольшее целое с условием $2^k\leqslant n$ и P — произведение всех нечётных чисел, не превосходящих n. Число $2^{k-1}PS$ представится суммою, все слагаемые которой, кроме $2^{k-1}P\frac{1}{2^s}$, суть целые числа.

b. Пусть k — наибольшее целое с условием $3^k\leqslant 2n+1$ и P — произведение всех взаимно простых с 6 чисел, не превосходящих $2n+1$. Число $3^{k-1}PS$ представится суммою, все слагаемые которой, кроме $3^{k-1}P\frac{1}{3^s}$, суть целые числа.

12. При $n\leqslant 8$ теорема проверяется непосредственно. Поэтому достаточно, считая при $n>8$ теорему верной для биномов $a+b$, $(a+b)^2,\dots,(a+b)^{n-1}$, доказать справедливость теоремы и для бинома $(a+b)^n$. Но коэффициенты разложения этого бинома за исключением крайних, равных 1, суть числа

$$\frac{n}{1},\ \frac{n(n-1)}{1\cdot 2},\dots,\frac{n(n-1)\dots 2}{1\cdot 2\dots(n-1)}.$$

Для нечётности же всех этих чисел необходимо и достаточно, чтобы нечётными были крайние из них, как раз равные n, и чтобы такие нечётными были числа, получаемые вычёркиванием нечётных сомножителей из числителей и знаменателей оставшихся чисел. Но, полагая $n=2n_1+1$, эти числа можно представить членами ряда

$$\frac{n_1}{1},\ \frac{n_1(n_1-1)}{1\cdot 2},\dots,\frac{n_1(n_1-1)\dots 2}{1\cdot 2\dots(n_1-1)}.$$

Последние же ввиду $n_1<n$ будут все нечётными тогда и только тогда, когда n_1 имеет вид 2^s-1, т. е. когда n имеет вид $2(2^s-1)+1=2^{s+1}-1$.

Решения к главе II.

1, a. На ординате точки кривой $y=f(x)$ с абсциссою x лежит $[f(x)]$ целых точек указанной области.

b. Указанное равенство следует из $T_1+T_2=T$, где T_1, T_2, T обозначают числа целых точек областей

$$0<x<\frac{Q}{2},\quad 0<y<\frac{P}{Q}x,$$

$$0<y<\frac{P}{2},\quad 0<x<\frac{Q}{P}y,$$

$$0<x<\frac{Q}{2},\quad 0<y<\frac{P}{2}.$$

c. Указанное равенство следует из

$$T=1+4(T_1+T_2+T_3-T_4),$$

где T_1, T_2, T_3, T_4 обозначают числа целых точек областей

$$x=0,\qquad 0<y\leqslant r;$$

$$0<x\leqslant\frac{r}{\sqrt{2}},\qquad 0<y\leqslant\sqrt{r^2-x^2};$$

$$0<y\leqslant\frac{r}{\sqrt{2}},\qquad 0<x\leqslant\sqrt{r^2-y^2};$$

$$0<x\leqslant\frac{r}{\sqrt{2}},\qquad 0<y\leqslant\frac{r}{\sqrt{2}}.$$

d. Указанное равенство следует из $T=T_1+T_2-T_3$, где T_1, T_2, T_3 обозначают числа целых точек областей

$$0<x\leqslant\sqrt{n},\quad 0<y\leqslant\frac{n}{x};$$

$$0<y\leqslant\sqrt{n},\quad 0<x\leqslant\frac{n}{y},$$

$$0<x\leqslant\sqrt{n},\quad 0<y\leqslant\sqrt{n}.$$

2. Число целых положительных чисел, не превосходящих n, равно $[n]$. Каждое из них единственным способом представляется в форме xk^m, где k — целое положительное; при этом данному x отвечает $\left[\sqrt[m]{\frac{n}{x}}\right]$ чисел такой формы.

3. Докажем необходимость указанных условий. Пусть N — целое, $N>1$. Число значений x с условием $[\alpha x]\leqslant N$ можно представить в форме $\frac{N}{\alpha}+\lambda$; $0\leqslant\lambda\leqslant C$, а число значений y с условием $[\beta y]\leqslant N$ можно представить в форме $\frac{N}{\beta}+\lambda_1$; $0\leqslant\lambda_1\leqslant C_1$, где C и C_1 не зависят от N. Из $\frac{N}{\alpha}+\lambda+\frac{N}{\beta}+\lambda_1=N$, деля на N и переходя к пределу при $N\to\infty$, получим $\frac{1}{\alpha}+\frac{1}{\beta}=1$. Последнее равенство при рациональном $\alpha=\frac{a}{b}$ $(a>b>0)$ дало бы $[ab]=[\beta(a-b)]$.

Пусть указанные условия выполнены. Пусть c — целое, $c>0$, $x_0=\frac{c}{\alpha}+\xi$ и $y_0=\frac{c}{\beta}+\eta$ — наименьшие целые с условиями $x_0>\frac{c}{\alpha}$, $y_0>\frac{c}{\beta}$. Очевидно, $[\alpha x]\gtrless c$ при $x\gtrless x_0$ и $[\beta y]\gtrless c$ при $y\gtrless y_0$, $0<\xi<1$, $0<\eta<1$, $\alpha\xi$ и $\beta\eta$ — иррациональные. Ввиду $x_0+y_0=c+\eta+\xi$ имеем $\xi+\eta=1$, $\frac{\alpha\xi}{\alpha}+\frac{\beta\eta}{\beta}=1$: поэтому одно и только одно из чисел $\alpha\xi$ и $\beta\eta$ меньше 1. Следовательно, одно и только одно из чисел $[\alpha x_0]$ и $[\beta y_0]$ равно c.

4, a. Указанные разности равны

$$\{\alpha x_1\},\ \{\alpha(x_2-x_1)\},\ \ldots,\ \{\alpha(x_t-x_{t-1})\},\ \{-\alpha x_t\},$$

они неотрицательные, их сумма равна 1, их число равно $t+1$; поэтому, по крайней мере, одна из этих разностей не превосходит $\frac{1}{t+1}<\frac{1}{\tau}$ и, таким образом, существует число, меньшее $\frac{1}{\tau}$, вида $\{\pm\alpha Q\}$, где $0<Q\leqslant\tau$. Из $\pm\alpha Q=[\pm\alpha Q]+\{\pm\alpha Q\}$, полагая $\pm[\pm\alpha Q]=P$, находим $|\alpha Q-P|<\frac{1}{\tau}$, $\left|\alpha-\frac{P}{Q}\right|<\frac{1}{Q\tau}$.

b. Полагая $X_0=[X]$, $Y_0=[Y]$, $\ldots$, $Z_0=[Z]$, рассмотрим ряд, образованный расположенными в неубывающем порядке числами вида $\{\alpha x+\beta y+\ldots+\gamma z\}$ и числом 1, предполагая, что x, y, $\ldots$, z пробегают значения:

$$x=0,\ 1,\ \ldots,\ X_0;\ y=0,\ 1,\ \ldots,\ Y_0;\ \ldots;\ z=0,\ 1,\ \ldots,\ Z_0.$$

Получим $(X_0+1)(Y_0+1)\ldots(Z_0+1)+1$ чисел, из которых составим $(X_0+1)(Y_0+1)\ldots(Z_0+1)$ разностей. По крайней мере, одна из этих разностей не превосходит

$$\frac{1}{(X_0+1)(Y_0+1)\ldots(Z_0+1)}<\frac{1}{XY\ldots Z}.$$

Отсюда уже легко получается указанная теорема.

5. Имеем $a = cq + r + (\alpha)$; $0 \leqslant r < q$,

$$\left[\frac{[\alpha]}{c}\right] = \left[q + \frac{r}{c}\right] = q, \quad \left[\frac{\alpha}{c}\right] = \left[q + \frac{r + (\alpha)}{c}\right] = q.$$

6, a. Имеем $[\alpha + \beta + \ldots + \lambda] = [\alpha] + [\beta] + \ldots + [\lambda] + [(\alpha) + (\beta) + \ldots + (\lambda)]$.

b. Простое p входит в $n!$, $a!$, $\ldots$, $l!$ с показателями

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots, \quad \left[\frac{a}{p}\right] + \left[\frac{a}{p^2}\right] + \ldots, \quad \ldots, \quad \left[\frac{l}{p}\right] + \left[\frac{l}{p^2}\right] + \ldots$$

При этом

$$\left[\frac{n}{p^s}\right] \geqslant \left[\frac{a}{p^s}\right] + \ldots + \left[\frac{l}{p^s}\right].$$

7. Допуская, что число a с указанными свойствами существует, представим его в форме

$$a = q_k p^{k+1} + q_{k-1} p^k + \ldots + q_1 p^2 + q_0 p + q';$$

$$0 < q_k < p, \quad 0 \leqslant q_{k-1} < p, \quad \ldots, \quad 0 \leqslant q_1 < p, \quad 0 \leqslant q_0 < p, \quad 0 \leqslant q' < p.$$

Согласно b, § 1 должно быть

$$h = q_k u_k + q_{k-1} u_{k-1} + \ldots + q_1 u_1 + q_0 u_0.$$

Далее при любом $s = 1, 2, \ldots, m$ имеем

$$q_{s-1} u_{s-2} + q_{s-2} u_{s-3} + \ldots + q_1 u_1 + q_0 u_0 < u_s.$$

Поэтому последнее выражение для h должно полностью совпасть с указанным в вопросе.

8, a. Пусть x_1 — целое, $Q \leqslant \alpha < \beta \leqslant R$, $x_1 < \alpha < \beta < x_1 + 1$; интегрированием по частям находим

$$-\int_\alpha^\beta f(x)\,dx = \int_\alpha^\beta \rho'(x) f(x)\,dx =$$

$$= \rho(\beta) f(\beta) - \rho(\alpha) f(\alpha) - \sigma(\beta) f'(\beta) + \sigma(\alpha) f'(\alpha) + \int_\alpha^\beta \sigma(x) f''(x)\,dx.$$

В частности, при $Q \leqslant x_1$, $x_1 + 1 \leqslant R$, переходя к пределу, имеем

$$-\int_{x_1}^{x_1+1} f(x)\,dx = -\frac{1}{2} f(x_1 + 1) - \frac{1}{2} f(x_1) + \int_{x_1}^{x_1+1} \sigma(x) f''(x)\,dx.$$

Указанная формула теперь получается без всякого труда.

b. Переписав формулу вопроса a в виде

$$\sum_{Q < x \leqslant R} f(x) = \int_R^Q f(x)\,dx - \int_R^Q f(x)\,dx + \rho(R) f(R) - \rho(Q) f(Q) -$$

$$- \sigma(R) f'(R) + \sigma(Q) f'(Q) + \int_Q^\infty \sigma(x) f''(x)\,dx - \int_R^\infty \sigma(x) f''(x)\,dx,$$

убеждаемся в справедливости указанной формулы.

c. Применяя результат вопроса b, находим

$$\ln 1 + \ln 2 + \ldots + \ln n = C + n \ln n - n + \frac{1}{2} \ln n + \int_n^\infty \frac{\sigma(x)}{x^2}\,dx =$$

$$= n \ln n - n + O(\ln n).$$

9, a. α) Имеем (b, § 1)

$$\ln([n]!) = \sum_{p \leqslant n} \left(\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots \right) \ln p. \tag{1}$$

Здесь правая часть представляет сумму значений функции $\ln p$, распространённую на целые точки (p, s, u) с простыми p области $p > 0$, $s > 0$, $0 < u \leqslant \frac{n}{p^s}$. Часть этой суммы, отвечающая данным s и u, равна $\Theta\left(\sqrt{\frac{n}{u}}\right)$, часть, отвечающая данному u, равна $\psi\left(\frac{n}{u}\right)$.

β) Применяя при $n \geqslant 2$ результат вопроса α), имеем

$$\ln([n]!) - 2 \ln\left(\left[\frac{n}{2}\right]!\right) =$$

$$= \psi(n) - \psi\left(\frac{n}{2}\right) + \psi\left(\frac{n}{3}\right) - \psi\left(\frac{n}{4}\right) + \ldots \geqslant \psi(n) - \psi\left(\frac{n}{2}\right).$$

Полагая $\left[\frac{n}{2}\right] = m$, отсюда находим ($[n] = 2m$, или $[n] = 2m + 1$)

$$\psi(n) - \psi\left(\frac{n}{2}\right) \leqslant \ln \frac{(2m+1)!}{(m!)^2} \leqslant \ln\left(2^m \frac{3 \cdot 5 \ldots (2m+1)}{1 \cdot 2 \ldots m}\right) \leqslant$$

$$\leqslant \ln(2^m 3^m) < n,$$

$$\psi(n) = \psi(n) - \psi\left(\frac{n}{2}\right) + \psi\left(\frac{n}{2}\right) - \psi\left(\frac{n}{4}\right) +$$

$$+ \psi\left(\frac{n}{4}\right) - \psi\left(\frac{n}{8}\right) + \ldots < n + \frac{n}{2} + \frac{n}{4} + \ldots = 2n.$$

γ) Имеем (решение вопроса β) и результат вопроса 8, c)

$$\gamma(n)-\gamma\left(\frac{n}{2}\right)+\gamma\left(\frac{n}{3}\right)-\gamma\left(\frac{n}{4}\right)+\ldots = \ln\frac{[n]!}{\left(\left[\frac{n}{2}\right]!\right)^2}=$$

$$=[n]\ln[n]-[n]-2\left[\frac{n}{2}\right]\ln\left[\frac{n}{2}\right]+2\left[\frac{n}{2}\right]+O(\ln n)=$$

$$=n\ln 2+O(\ln n).$$

Далее, при $s\geqslant 2$ находим (вопрос β))

$$\Theta\left(\sqrt[s]{n}\right)-\Theta\left(\sqrt[s]{\frac{n}{2}}\right)+$$

$$+\Theta\left(\sqrt[s]{\frac{n}{3}}\right)-\ldots\begin{cases}<2\sqrt{n} \text{ всегда}\\ =0 \text{ при } s>\tau;\ \tau=\left[\frac{\ln n}{\ln 2}\right].\end{cases}$$

Поэтому

$$0\leqslant\gamma(n)-\gamma\left(\frac{n}{2}\right)+\gamma\left(\frac{n}{3}\right)-\gamma\left(\frac{n}{4}\right)+$$

$$+\ldots-\left(\Theta(n)-\Theta\left(\frac{n}{2}\right)+\Theta\left(\frac{n}{3}\right)-\Theta\left(\frac{n}{4}\right)+\ldots\right)<$$

$$<2\sqrt{n}+2\sqrt[3]{n}+2\sqrt[4]{n}+\ldots+2\sqrt[\tau]{n}<2\left(\sqrt{n}+\tau\sqrt[3]{n}\right)=O\left(\sqrt{n}\right).$$

b. Следует из равенства (1), неравенства вопроса a, β) и равенства вопроса 8, c.

c. Равенство вопроса b при достаточно больших m дает

$$\sum_{m<p\leqslant m^2}\frac{\ln p}{p}=\ln m+O(1)\geqslant\frac{\ln m}{2},\qquad \sum_{m<p\leqslant m^2}\frac{4}{p}>1.$$

Если для всех пар p_n, p_{n+1} с условием $m<p_n<p_{n+1}\leqslant m^2$ имело бы место неравенство $p_{n+1}>p_n(1+\varepsilon)$, то было бы

$$\sum_{r=0}^{\infty}\frac{4}{m(1+\varepsilon)^r}>1,$$

что при достаточно больших m невозможно.

d. Очевидно достаточно рассматривать лишь случай, когда n — целое.

Полагая $\gamma(r)=\dfrac{\ln r}{r}$ при r простом и $\gamma(r)=0$ при $r=1$, или при r составном, имеем (вопрос b)

$$\gamma(1)+\gamma(2)+\ldots+\gamma(r)=\ln r+\alpha(r);\quad |\alpha(r)|<C_1,$$

где C_1 — постоянное. Отсюда при $r>1$ (считаем $\alpha(1)=1$)

$$\gamma(r)=\ln r-\ln(r-1)+\alpha(r)-\alpha(r-1),$$

$$\sum_{0<p\leqslant n}\frac{1}{p}=T_1+T_2;\quad T_1=\sum_{1<r\leqslant n}\frac{\ln r-\ln(r-1)}{\ln r},$$

$$T_2=\sum_{1<r\leqslant n}\frac{\alpha(r)-\alpha(r-1)}{\ln r}.$$

Имеем (8, b)

$$T_1=\sum_{1<r\leqslant n}\frac{1}{r\ln r}+\sum_{1<r\leqslant n}\left(\frac{1}{2r^2\ln r}+\frac{1}{3r^3\ln r}+\ldots\right)=$$

$$=C_2+\ln\ln n+O\left(\frac{1}{\ln n}\right),$$

где C_2 — постоянное. Далее находим

$$T_2=\alpha(2)\left(\frac{1}{\ln 2}-\frac{1}{\ln 3}\right)+\ldots+\alpha(n-1)\left(\frac{1}{\ln(n-1)}-\frac{1}{\ln n}\right)+\frac{\alpha(n)}{\ln n}.$$

Но при целом $m>1$ имеем

$$C_1\left(\frac{1}{\ln m}-\frac{1}{\ln(m+1)}\right)+C_1\left(\frac{1}{\ln(m+1)}-\frac{1}{\ln(m+2)}\right)+\ldots=\frac{C_1}{\ln m}.$$

Поэтому ряд

$$\alpha(2)\left(\frac{1}{\ln 2}-\frac{1}{\ln 3}\right)+\alpha(3)\left(\frac{1}{\ln 3}-\frac{1}{\ln 4}\right)+\ldots$$

сходится; при этом, если C_3 его сумма, то

$$T_2=C_3+O\left(\frac{1}{\ln n}\right).$$

e. Имеем

$$\ln\prod\left(1-\frac{1}{p}\right)=-\sum_{p\leqslant n}\frac{1}{p}-\sum_{p\leqslant n}\left(\frac{1}{2p^2}+\frac{1}{2p^3}+\ldots\right)=$$

$$=C'-\ln\ln n+O\left(\frac{1}{\ln n}\right),$$

где C' — постоянное. Отсюда, полагая $C'=\ln C_4$, мы и получим указанное равенство.

10, a. Следует из c, § 2.

b. Ввиду $\vartheta(1)=\gamma(1)=1$ условие 1, a, § 2 для функции $\vartheta(a)$ выполнено. Пусть $a=a_1a_2$ — одно из разложений a на два взаимно простых сомножителя. Имеем

$$\sum_{d_1\mid a_1}\sum_{d_2\mid a_2}\vartheta(d_1d_2)=\gamma(a)=\gamma(a_1)\gamma(a_2)=\sum_{d_1\mid a_1}\sum_{d_2\mid a_2}\vartheta(d_1)\vartheta(d_2).\quad(1)$$

Если условие 2, а, § 2 выполнено для всех произведений, меньших a, то при $d_1 d_2 < a$ имеем $\theta(d_1 d_2) = \theta(d_1)\,\theta(d_2)$, и равенство (1) даёт $\theta(a_1 a_2) = \theta(a_1)\,\theta(a_2)$, т. е. условие 2, а, § 2 выполняется и для всех произведений $a_1 a_2$, равных a. Но условие 2, а, § 2 выполняется для единственного произведения $1 \cdot 1$, равного 1. Следовательно, оно выполняется и для всех произведений.

11, а. Пусть $m > 1$; для каждого данного x_m, делящего a, неопределённое уравнение $x_1 \dots x_{m-1} x_m = a$ имеет $\tau_{m-1}\left(\frac{a}{x_m}\right)$ решений. Поэтому

$$\tau_m(a) = \sum_{x_m \setminus a} \tau_{m-1}\left(\frac{a}{x_m}\right),$$

но когда x_m пробегает все делители числа a, то $d = \frac{a}{x_m}$ в обратном порядке пробегает те же делители. Следовательно,

$$\tau_m(a) = \sum_{d \setminus a} \tau_{m-1}(a).$$

Поэтому (вопрос 10, а) если теорема верна для функции $\tau_{m-1}(a)$, то она верна и для функции $\tau_m(a)$. Но теорема верна для функции $\tau_1(a) = 1$. Значит, она верна всегда.

b. Если $m > 1$ и теорема верна для функции $\tau_{m-1}(a)$, то имеем

$$\tau_m(a) = \tau_m(p_1) \dots \tau_m(p_k) =$$
$$= (\tau_{m-1}(1) + \tau_{m-1}(p_1)) \dots (\tau_{m-1}(1) + \tau_{m-1}(p_k)) = (1 + m - 1)^k = m^k.$$

Но теорема верна для функции $\tau_1(a)$. Значит, она верна всегда.

c. Пусть $\varepsilon = m^{-2}$, $\varepsilon_2 = 2\eta$, $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ — каноническое разложение числа a, причём $p_1, \dots, p_k$ расположены в возрастающем порядке. Для функции $\tau_2(a) = \tau(a)$ имеем

$$\frac{\tau(a)}{a^\eta} \leqslant \frac{\alpha_1 + 1}{2^{\alpha_1 \eta}} \frac{\alpha_2 + 1}{3^{\alpha_2 \eta}} \dots \frac{\alpha_k + 1}{(k+1)^{\alpha_k \eta}}.$$

Каждый из сомножителей произведения, стоящего справа, меньше $\frac{1}{\eta}$; сомножители $\frac{\alpha_{r-1} + 1}{r^{\alpha_{r-1}\eta}}$ с условием $r > 2^{\frac{1}{\eta}}$ меньше $\frac{\alpha_{r-1} + 1}{2^{\alpha_{r-1}}} \leqslant 1$. Поэтому, полагая $C = \left(\frac{1}{\eta}\right)^{2^{\frac{1}{\eta}}}$, находим

$$\frac{\tau(a)}{a^\eta} < C, \quad \lim_{a \to \infty} \frac{\tau(a)}{a^{\varepsilon_2}} \leqslant \lim_{a \to \infty} \frac{C}{a^\eta} = 0.$$

При $m > 2$, очевидно, имеем $\tau_m(a) \leqslant (\tau(a))^m$. Поэтому

$$\lim_{a \to \infty} \frac{\tau_m(a)}{a^\varepsilon} \leqslant \lim \left(\frac{\tau(a)}{a^{\varepsilon_2}}\right)^m = 0.$$

d. Системы значений $x_1, \dots, x_m$, удовлетворяющие указанному неравенству, разобьём на $[n]$ совокупностей с номерами $1, 2, \dots, [n]$. К совокупности с номером a отнесём системы с условием $x_1 \dots x_m = a$; число этих систем есть $\tau_m(a)$.

12. При $R(s) > 1$ ряд, выражающий $\zeta(s)$, абсолютно сходится. Поэтому

$$(\zeta(s))^m = \sum_{n_1=1}^{\infty} \dots \sum_{n_m=1}^{\infty} \frac{1}{(n_1 \dots n_m)^s},$$

причём при данном положительном n число систем $n_1, \dots, n_m$ с условием $n_1 \dots n_m = n$ равно $\tau_m(n)$.

13, а. При $R(s) > 1$ произведение $P = \prod_p \frac{1}{1 - \frac{1}{p^s}}$ абсолютно сходится. Ввиду $\frac{1}{1 - \frac{1}{p^s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots$ при $N > 2$ имеем

$$\prod_{p \leqslant N} \frac{1}{1 - \frac{1}{p^s}} = \sum_{0 < n \leqslant N} \frac{1}{n^s} + \sum' \frac{1}{n^s},$$

где во второй сумме правой части n пробегает лишь числа, не делящиеся на простые, превосходящие N. В пределе при $N \to \infty$ левая часть обратится в P, первая сумма правой части — в $\zeta(s)$, вторая — в нуль.

b. Пусть $N > 2$. Допустив, что простых чисел, отличных от $p_1, \dots, p_k$, нет, находим (ср. решение вопроса а)

$$\prod_{j=1}^{k} \frac{1}{1 - \frac{1}{p_j}} \geqslant \sum_{0 < n \leqslant N} \frac{1}{n},$$

Это неравенство ввиду расходимости гармонического ряда $1 + \frac{1}{2} + \frac{1}{3} + \dots$ при достаточно больших N невозможно.

c. Допустив, что простых чисел, отличных от $p_1, \ldots, p_k$ нет, находим (вопрос a)

$$\prod_{j=1}^{k} \frac{1}{1-\frac{1}{p_j^2}} = \zeta(2).$$

Это равенство ввиду иррациональности $\zeta(2) = \frac{\pi^2}{6}$ невозможно.

14. При $R(s) > 1$ бесконечное произведение для $\zeta(s)$ вопроса 13, a абсолютно сходится. Поэтому

$$\ln \zeta(s) = \sum_p \left(\frac{1}{p^s} + \frac{1}{2p^{2s}} + \frac{1}{3p^{3s}} + \ldots \right),$$

где p пробегает все простые числа. Дифференцируя, имеем

$$\frac{\zeta'(s)}{\zeta(s)} = \sum_p \left(-\frac{\ln p}{p^s} - \frac{\ln p}{p^{2s}} - \frac{\ln p}{p^{3s}} - \ldots \right) = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

15. Пусть $N > 2$. Применяя теорему b, § 3, имеем

$$\prod_{p \leqslant N} \left(1 - \frac{1}{p^s}\right) = \sum_{0 < n \leqslant N} \frac{\mu(n)}{n^s} + \sum' \frac{\mu(n)}{n^s},$$

где во второй сумме правой части n пробегает лишь числа, большие N и не делящиеся на простые, превосходящие N. В пределе при $N \to \infty$ мы и получим указанное тождество.

16. a. Применим d, § 3 к случаю

$$\delta = 1, 2, \ldots, [n], \quad f = 1, 1, \ldots, 1.$$

Тогда, очевидно, $S' = 1$. Далее S_d обращается в число значений δ, кратных d, т. е. в $\left[\frac{n}{d}\right]$.

b. α) Правая часть равенства вопроса a выражает сумму значений функции $\mu(d)$, распространённую на целые точки (d, u) области $d > 0$, $0 < u \leqslant \frac{n}{d}$. Часть этой суммы, отвечающая данному u, равна $M\left(\frac{n}{u}\right)$.

β) Указанное равенство получается почленным вычитанием равенств

$$M(n) + M\left(\frac{n}{2}\right) + M\left(\frac{n}{3}\right) + M\left(\frac{n}{4}\right) + \ldots = 1,$$

$$2M\left(\frac{n}{2}\right) + \qquad 2M\left(\frac{n}{4}\right) + \ldots = 2.$$

c. Пусть $n_1 = [n]$; $\delta_1, \delta_2, \ldots, \delta_n$ определяются условием: δ_x есть наибольшее целое, l-я степень которого делит s, $f_x = 1$. Тогда $S' = T_{l,n}$. S_d равно числу чисел, не превосходящих n, кратных d^l, т. е. $S_d = \left[\frac{n}{d^l}\right]$. Отсюда получается указанное выражение для $T_{l,n}$.

В частности, ввиду $\zeta(2) = \frac{\pi^2}{6}$ для числа $T_{2,n}$ чисел, не превосходящих n и не делящихся на квадрат целого, превосходящего 1, имеем

$$T_{2,n} = \frac{6}{\pi^2} n + O(\sqrt{n}).$$

17, a. Указанное равенство получим из d, § 3, если положим

$$\delta_x = (x_1, a), \quad f_x = f(x_1).$$

b. Указанное равенство получим из d, § 3, если положим

$$\delta_x = (x_1^{(s)}, \ldots, x_k^{(s)}), \quad f_x = f(x_1^{(s)}, \ldots, x_k^{(s)}).$$

c. Применяя d, § 3 к случаю

$$\delta = \delta_1, \delta_2, \ldots, \delta_\tau,$$

$$f = F\left(\frac{a}{\delta_1}\right), \quad F\left(\frac{a}{\delta_2}\right), \ldots, F\left(\frac{a}{\delta_\tau}\right),$$

где в первой строке выписаны все делители числа a, имеем

$$S' = F(a), \quad S_d = \sum_{D \backslash \frac{a}{d}} F\left(\frac{a}{dD}\right) = G\left(\frac{a}{d}\right).$$

d. Указанное равенство следует из

$$P' = f_1^{\sum_{d \backslash \delta_1} \mu(d)} \; f_2^{\sum_{d \backslash \delta_2} \mu(d)} \ldots f_n^{\sum_{d \backslash \delta_n} \mu(d)}.$$

18, a. Применим теорему вопроса 17, a, заставляя x пробегать числа $1, 2, \ldots, a$ и беря $f(x) = x^m$. Тогда

$$S' = \psi_m(a), \quad S_d = d^m + 2^m d^m + \ldots + \left(\frac{a}{d}\right)^m d^m = d^m \sigma_m\left(\frac{a}{d}\right).$$

b. Имеем

$$\psi_1(a) = \sum_{d \backslash a} \mu(d) \left(\frac{a^2}{2d} + \frac{a}{2}\right) = \frac{a}{2} \varphi(a).$$

Тот же результат можно получить проще. Напишем числа ряда $1, \ldots, a$, взаимно простые с a сначала в возрастающем, затем

в убывающем порядке. Сумма членов обоих рядов, равноотстоящих от начала, равна a; число членов каждого ряда равно $\varphi(a)$.

c. Имеем

$$\psi_2(a)=\sum_{d\setminus a}\mu(d)\left(\frac{a^3}{3d}+\frac{a^2}{2}+\frac{a}{6}d\right)=\frac{a^2}{3}\varphi(a)+\frac{a}{6}(1-p_1)\dots(1-p_k).$$

19, a. Применим теорему вопроса 17, a, заставляя x пробегать числа $1, 2, \dots, [z]$ и беря $f(x)=1$. Тогда $S'=T_z$, S_d равно числу чисел, не превосходящих z, кратных d, т. е. $S_d=\left[\frac{z}{d}\right]$.

b. Имеем

$$T_z=\sum_{d\setminus a}\mu(d)\frac{z}{d}+O(\tau(a))=\frac{z}{a}\varphi(a)+O(a^\varepsilon).$$

c. Следует из равенства вопроса a.

20. Применим теорему вопроса 17, a, заставляя x пробегать числа $1, 2, \dots, N$, где $N>a$, и беря $f(x)=\frac{1}{x^s}$. Тогда найдём

$$\sum_{x\leqslant N}{}'\frac{1}{x^s}=\sum_{d\setminus a}\mu(d)\sum_{1<x\leqslant\frac{N}{d}}\frac{1}{d^s x^s}=\sum_{d\setminus a}\frac{\mu(d)}{d^s}\sum_{0<x\leqslant\frac{N}{d}}\frac{1}{x^s}$$

В пределе при $N\to\infty$ получим указанное тождество.

21, a. Применим теорему вопроса 17, b, рассматривая указанные в определении вероятности P_N системы значений $x_1, x_2, \dots, x_k$ и беря $f(x_1, x_2, \dots, x_k)=1$. Тогда $P_N=\frac{S'}{N^k}$, $S_d=\left[\frac{N}{d}\right]^k$, и мы получим

$$P_N=\frac{\sum_{d=1}^{N}\mu(d)\left[\frac{N}{d}\right]^k}{N^k}=\sum_{d=1}^{N}\frac{\mu(d)}{d^k}+O\left(\sum_{d=1}^{N}\frac{1}{Nd^{k-1}}\right).$$

Поэтому

$$P_N=(\zeta(k))^{-1}+O(\Delta);\quad \Delta=\frac{1}{N}\text{ при }k>2,\quad \Delta=\frac{\ln N}{N}\text{ при }k=2.$$

b. Имеем $\zeta(2)=\frac{\pi^2}{6}$.

22, a. Элементарные рассуждения показывают, что число целых точек (u, v) области $u^2+v^2\leqslant\rho^2$; $\rho>0$, не считая точки $(0, 0)$, равно $\pi\rho^2+O(\rho)$. Применим теорему вопроса 17, b, рассматривая координаты x, y целых точек области $x^2+y^2\leqslant r^2$, отличных от точки $(0, 0)$, и полагая $f(x, y)=1$. Тогда $T=S'+1$, S_d равно числу целых точек области $u^2+v^2\leqslant\left(\frac{r}{d}\right)^2$, не считая точки $(0, 0)$. Поэтому

$$S_d=\pi\frac{r^2}{d^2}+O\left(\frac{r}{d}\right),$$

$$T=\sum_{d=1}^{[r]}\mu(d)\,\pi\frac{r^2}{d^2}+O\left(\sum_{d=1}^{[r]}\frac{r}{d}\right)=\frac{6}{\pi}r^2+O(r\ln r).$$

b. Рассуждая аналогично предыдущему, получим

$$T=\sum_{d=1}^{[r]}\mu(d)\,\frac{4}{3}\pi\frac{r^3}{d^3}+O\left(\sum_{d=1}^{[r]}\frac{r^2}{d^2}\right)=\frac{4\pi r^3}{3\zeta(3)}+O(r^2).$$

23. a. Число делителей d числа $a=p_1^{\alpha_1}\dots p_k^{\alpha_k}$, не делящихся на квадрат целого, превосходящего 1, и имеющих $\varkappa$ простых делителей, равно $\binom{k}{\varkappa}$; при этом $\mu(d)=(-1)^\varkappa$. Поэтому

$$\sum_{d\setminus a}\mu(d)=\sum_{\varkappa=0}^{k}\binom{k}{\varkappa}(-1)^\varkappa=(1-1)^k=0.$$

b. Пусть a имеет тот же вид, что и в вопросе a. Достаточно рассматривать случай $m<k$. Для указанной суммы имеем два выражения

$$\sum\mu(d)=\binom{k}{0}-\binom{k}{1}+\dots+(-1)^m\binom{k}{m}=$$
$$=(-1)^m\left(\binom{k}{m+1}-\binom{k}{m+2}+\dots\right).$$

Если m чётное, то при $m\leqslant\frac{k}{2}$ первое выражение >0, а при $m>\frac{k}{2}$ второе выражение $\geqslant 0$. Если m нечётное, то при $m\leqslant\frac{k}{2}$ первое выражение <0, а при $m>\frac{k}{2}$ второе выражение $\leqslant 0$.

c. Доказательство почти такое же, как в d, § 3, но с учётом результата вопроса b.

d. Доказательство почти такое же, как в вопросах 17, a и 17, b

24. Пусть d пробегает делители числа a, $\Omega(d)$ — число простых делителей числа d, $\omega(a)=s$. Согласно сделанному в вопросе указанию, имеем (считаем N достаточно большим)

$$\pi(N, q, l) \leqslant \sum_{\Omega(d)\leqslant m} \mu(d)\left(\frac{N}{qd}+\theta_d\right) = T + T_0 - T_1; \quad |\theta_d| \leqslant 1,$$

$$|T| \leqslant \sum_{\Omega(d)\leqslant m} 1, \quad T_0 = \frac{N}{q}\sum_{d}\frac{\mu(d)}{d}, \quad |T_1| = \sum_{\Omega(d)>m}\frac{N}{qd}.$$

Далее находим

$$|T| \leqslant \sum_{n=0}^{m}\binom{s}{n} \leqslant s^m \leqslant e^{hm} < e^{5r^{1-\varepsilon}\ln r}\frac{q^r}{N}\frac{N}{q^r} = O(1),$$

$$T_0 = \frac{N}{q}\frac{\prod_{p\leqslant e^h}\left(1-\frac{1}{p}\right)}{\prod_{p\mid q}\left(1-\frac{1}{p}\right)} = O(1).$$

Наконец, обозначая буквами C_1 и C_2 некоторые постоянные, имеем

$$|T_1| \leqslant \frac{N}{q}\sum_{n=m+1}^{s}\sum_{\Omega(d)=n}\frac{1}{d} \leqslant \frac{N}{q}\sum_{n=m+1}^{s}\frac{\left(\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{p_s}\right)^n}{n!} \leqslant$$

$$\leqslant \frac{N}{q}\sum_{n=m+1}^{s}\left(\frac{C_1+\ln r}{4\ln r}e\right)^n \leqslant$$

$$\leqslant \frac{N}{q}\sum_{n=m+1}^{s}\left(\frac{3}{4}\right)^n < C_2\frac{N}{q}r^{-4\ln\frac{4}{3}} = O(1).$$

25. Всякому делителю d_1 числа a с условием $d_1 < \sqrt{a}$ отвечает делитель d_2 с условиями $d_2 > \sqrt{a}$, $d_1 d_2 = a$. При этом $\mu(d_1) = -\mu(d_2)$. Поэтому

$$2\sum_{d_1}\mu(d_1) = \sum_{d_1}\mu(d_1) + \sum_{d_2}\mu(d_2) = \sum_{d\mid a}\mu(d) = 0.$$

26. Числа d, не делящиеся на квадрат целого, превосходящего 1, и удовлетворяющие условию $\varphi(d)=k$, рассмотрим попарно так, чтобы в каждую пару входило некоторое нечётное d_1 и чётное $2d_1$. Будем иметь $\mu(d_1)\cdot\mu(2d_1)=0$.

27. Пусть $p_1, \ldots, p_k$ — различные простые числа. Полагая $a = p_1 \ldots p_k$, имеем

$$\varphi(a) = (p_1-1)\ldots(p_k-1).$$

Между тем, при отсутствии простых чисел, отличных от $p_1, \ldots, p_k$, мы имели бы $\varphi(a)=1$.

28. a. Указанные числа найдутся среди чисел $s\delta$: $s = 1, 2, \ldots, \frac{a}{\delta}$. Но $(s\delta, a) = \delta$ тогда и только тогда, когда $\left(s, \frac{a}{\delta}\right) = 1$ (e, § 2, гл. I). Поэтому верно утверждение, отмеченное в вопросе, и мы имеем

$$a = \sum_{d\mid a}\varphi\left(\frac{a}{\delta}\right) = \sum_{d\mid a}\varphi(d).$$

b, α) Пусть $a = p_1^{\alpha_1}\ldots p_k^{\alpha_k}$ — каноническое разложение числа a. Ввиду а функция $\varphi(a)$ мультипликативная, причём

$$p_s^{\alpha_s} = \sum_{d\mid p_s^{\alpha_s}}\varphi(d), \qquad p_s^{\alpha_s-1} = \sum_{d\mid p_s^{\alpha_s-1}}\varphi(d), \qquad p_s^{\alpha_s} - p_s^{\alpha_s-1} = \varphi(p_s^{\alpha_s}).$$

β) Для целого $m > 0$ имеем

$$m = \sum_{d\mid m}\varphi(d).$$

Поэтому

$$\varphi(a) = \sum_{d\mid a}\mu(d)\frac{a}{d}.$$

29. Имеем (p пробегает все простые числа)

$$\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s} = \prod_{p}\left(1+\frac{\varphi(p)}{p^s}+\frac{\varphi(p^2)}{p^{2s}}+\ldots\right) = \prod_{p}\frac{1-\frac{1}{p^s}}{1-\frac{1}{p^{s-1}}} = \frac{\zeta(s-1)}{\zeta(s)}.$$

30. Имеем

$$\varphi(1)+\varphi(2)+\ldots+\varphi(n)=\sum_{d\backslash 1}\frac{\mu(d)}{d}+2\sum_{d\backslash 2}\frac{\mu(d)}{d}+\ldots+n\sum_{d\backslash n}\frac{\mu(d)}{d}=$$

$$=\sum_{d=1}^{n}\mu(d)\left(1+2+\ldots+\left[\frac{n}{d}\right]\right)=\sum_{d=1}^{n}\mu(d)\,\frac{n^2}{2d^2}+O(n\ln n)=$$

$$=\frac{n^2}{2}\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}+O(n\ln n)=\frac{3}{\pi^2}n^2+O(n\ln n).$$

Решения к главе III.

1, a. Из

$$P=a_n 10^{n-1}+a_{n-1}10^{n-2}+\ldots+a_1,$$

замечая, что $10\equiv 1 \pmod 9$, имеем

$$P\equiv a_n+a_{n-1}+\ldots+a_1 \pmod 9.$$

Следовательно, P кратно 3 тогда и только тогда, когда сумма цифр, его изображающих, кратна 3; оно кратно 9 тогда и только тогда, когда указанная сумма кратна 9

Замечая, что $10\equiv -1 \pmod{11}$, имеем

$$P\equiv(a_1+a_3+\ldots)-(a_2+a_4+\ldots) \pmod{11}.$$

Следовательно, P кратно 11 тогда и только тогда, когда разность между суммою цифр, стоящих на нечётных (считая справа) местах, и суммою цифр, стоящих на чётных местах, кратна 11.

b. Из

$$P=b_n 100^{n-1}+b_{n-1}100^{n-2}+\ldots+b_1$$

ввиду $100\equiv -1 \pmod{101}$ имеем

$$P\equiv(b_1+b_3+\ldots)-(b_2+b_4+\ldots) \pmod{101}.$$

Поэтому P кратно 101 тогда и только тогда, когда $(b_1+b_3+\ldots)-(b_2+b_4+\ldots)$ кратно 101.

c. Из

$$P=c_n 1000^{n-1}+c_{n-1}1000^{n-2}+\ldots+c_1$$

ввиду $1000\equiv 1 \pmod{37}$ имеем

$$P\equiv c_n+c_{n-1}+\ldots+c_1 \pmod{37}.$$

Поэтому P кратно 37 тогда и только тогда, когда $c_n+c_{n-1}+\ldots+c_1$ кратно 37.

Ввиду $1000\equiv -1 \pmod{7\cdot 11\cdot 13}$ имеем

$$P\equiv(c_1+c_3+\ldots)-(c_2+c_4+\ldots) \pmod{7\cdot 11\cdot 13}.$$

Поэтому P кратно одного из чисел 7, 11, 13 тогда и только тогда, когда $(c_1+c_3+\ldots)-(c_2+c_4+\ldots)$ кратно этого же числа.

2, a. γ) Когда x пробегает полную систему вычетов по модулю m, то $ax-b$ также пробегает полную систему; наименьший неотрицательный вычет r числа $ax+b$ пробегает значения $0, 1, \ldots, m-1$. Поэтому

$$\sum_x\left\{\frac{ax+b}{m}\right\}=\sum_{r=0}^{m-1}\frac{r}{m}=\frac{1}{2}(m-1).$$

β) Применяя результат вопроса 18, b, гл. II, находим

$$\sum_{\xi}\left\{\frac{a\xi}{m}\right\}=\frac{\psi_1(m)}{m}=\frac{1}{2}\varphi(m).$$

b. В случае $t=1$ имеем $[f(N+m)]-[f(N)]=a$,

$$\sum\delta=\sum_{x=N+1}^{N+m}[f(x)]-\frac{1}{2}[f(N+m)]+\frac{1}{2}[f(N)]-\frac{1}{2}+\frac{1}{2}m=$$

$$=\sum_{x=N+1}^{N+m}f(x)-\sum_{x=N+1}^{N+m}\{f(x)\}-\frac{1}{2}a+\frac{1}{2}(m-1)=S;$$

к этому случаю тривиально сводится и случай $t>1$

c. Пусть N, M, P_1, P_2 — целые, $M>0$, $P_1>0$, $P_2>0$. Трапеции с вершинами $(N, 0)$, (N, P_1), $(N+M, 0)$, $(N+M, P_2)$ является частным случаем рассмотренной в вопросе b. Поэтому и для неё верно равенство (1). Равенство (1) для такой трапеции легко получим также, рассматривая прямоугольник с вершинами $(N, 0)$, (N, P_1+P_2), $(N+M, 0)$, $(N+M, P_1+P_2)$, равновеликий двум таким трапециям. Для этого прямоугольника равенство

$$\sum{}'\delta=S',$$

аналогичное равенству (1), очевидно. Отсюда ввиду $\sum'\delta=2\sum\delta$ $S'=2S$ мы и получим равенство (1).

Из этого результата аналогичная формула для указанного в вопросе треугольника выводится тривиально. Однако представляет интерес также следующий вывод: указанный треугольник получается путём разбиения на два равных треугольника некоторого параллелограмма с целыми вершинами. Пусть S — площадь параллелограмма и $T=\sum\delta$, где суммирование распространяется

на все целые точки параллелограмма, причём δ определяется аналогично тому, как в вопросе b. Интересующее нас свойство треугольника будет доказано, если мы докажем, что $S=T$. Рассмотрим квадрат с беспредельно растущей стороной A. Вся плоскость может быть разбита на бесчисленное множество параллелограммов указанного вида. Пусть k — число параллелограммов, полностью лежащих внутри квадрата и R — число целых точек внутри квадрата. При $A\to\infty$ находим

$$\lim\frac{kS}{A^2}=1,\quad \lim\frac{A^2}{R}=1,\quad \lim\frac{R}{kT}=1.$$

Перемножая почленно эти равенства, получим

$$\lim\frac{S}{T}=1,\quad S=T.$$

3, a. Пусть r — наименьший неотрицательный вычет числа $ax+[c]$ по модулю m. Имеем

$$S=\sum_{r=0}^{m-1}\left\{\frac{r+\Phi(r)}{m}\right\},$$

где $\varepsilon\leqslant\Phi(r)\leqslant\varepsilon+h$; $\varepsilon=\{c\}$. При $m\leqslant 2h+1$ теорема очевидна. Поэтому рассмотрим лишь случай $m>2h+1$. Полагая

$$\left\{\frac{r+\Phi(r)}{m}\right\}-\frac{r}{m}=\delta(r),$$

имеем $-1+\frac{\varepsilon}{m}\leqslant\delta(r)\leqslant\frac{h+\varepsilon}{m}$ при $r=m-[h+\varepsilon],\ \ldots,\ m-1$; $\frac{\varepsilon}{m}\leqslant\delta(r)\leqslant\frac{h+\varepsilon}{m}$ в остальных случаях. Поэтому

$$-[h+\varepsilon]+\varepsilon\leqslant S-\frac{m-1}{2}\leqslant h+\varepsilon,\quad \left|S-\frac{1}{2}m\right|\leqslant h+\frac{1}{2}.$$

b. Имеем

$$S=\sum_{z=0}^{m-1}\left\{\frac{az+\psi(z)}{m}\right\};\quad \psi(z)=m(AM+B)+\frac{\lambda}{m}z.$$

Применим теорему вопроса a, полагая $h=|\lambda|$. Тогда и получим указанный результат.

c. Находим

$$\sum_{z=0}^{m-1}\left\{f(M)+\frac{az}{m}+\frac{\theta z}{m^2}+\frac{f''(M+z_0)}{2}z^2\right\};\qquad 0<z_0<m-1.$$

Применим теорему вопроса a, полагая $h=1+\frac{k}{2}$. Тогда получим указанный результат.

4. Разложим A в непрерывную дробь. Пусть $Q_n=Q'$ — наибольший из знаменателей подходящих дробей, не превосходящий m, имеем (вопрос 4, b, гл I)

$$A=\frac{P'}{Q'}+\frac{\theta'}{Q'm},\quad (P',\ Q')=1,\ |\theta'|<1.$$

При этом из $m<Q_{n+1}\leqslant(q_{n+1}+1)Q_n\leqslant CQ_n$, где C — постоянное, которого не превосходят все q_s+1, для наибольшего целого H' с условием $H'Q'\leqslant m$ следует $H'<C$. Применяя теорему вопроса 3, b, находим

$$\left|\sum_{x=M}^{M+H'Q'-1}\{Ax+B\}-\frac{1}{2}H'Q'\right|\leqslant\frac{3}{2}C.$$

Пусть $m_1=m-H'Q'$. Если $m_1>0$, то, выбирая в зависимости от m_1 числа Q'' и H'' таким же способом, как раньше в зависимости от m были выбраны числа Q' и H', найдём

$$\sum_{x=M_1}^{M_1+H''Q''-1}\left|\{Ax+B\}-\frac{1}{2}H''Q''\right|\leqslant\frac{3}{2}C.$$

Пусть $m_2=m_1-H''Q''$. Если $m_2>0$, то подобно предыдущему найдём

$$\left|\sum_{x=M_2}^{M_2+H'''Q'''-1}\{Ax+B\}-\frac{1}{2}H'''Q'''\right|<\frac{3}{2}C$$

и т. д., пока не придём к некоторому $m_k=0$. Тогда получим $(H'Q'+H''Q''+\ldots+H^{(k)}Q^{(k)}=m)$

$$\left|\sum_{x=M}^{M+m-1}\{Ax+B\}-\frac{1}{2}m\right|<\frac{3}{2}Ck.$$

Числа $Q',\ Q'',\ \ldots,\ Q^{(k)}$ удовлетворяют условиям

$$m\geqslant Q'>m_1\geqslant Q''>m_2\geqslant\ldots>m_{k-1}\geqslant Q^{(k)}\geqslant 1.$$

Поэтому (вопрос 3, гл. I) $k=O(\ln m)$ и, следовательно, формула, указанная в вопросе, верна.

5, a. Сумму, стоящую слева, обозначим буквою S. Пусть $\tau = A^{\frac{1}{3}}$. При $\tau \leqslant 40$ теорема очевидна. Поэтому предполагаем $\tau > 40$. Взяв $M_1 = [Q+1]$, найдём числа a_1, m_1, θ_1 с условиями

$$f'(M_1) = \frac{a_1}{m_1} + \frac{\theta_1}{m_1 \tau}; \quad 0 < m \leqslant \tau, \quad (a_1, m_1) = 1, \quad |\theta_1| < 1.$$

Взяв $M_2 = M_1 + m_1$, аналогичным путём найдём числа a_2, m_2, θ_2; взяв $M_3 = M_2 + m_2$, найдём числа a_3, m_3, θ_3; и т. д., пока не придём к $M_{s+1} = M_s + m_s$ с условием $0 \leqslant [R] - M_{s+1} < [\tau]$. Применяя теорему вопроса 3, c, найдём

$$\left| S - \frac{1}{2}(m_1 + m_2 + \ldots + m_s + [R] - M_{s+1}) \right| < s\frac{k+3}{2} + \frac{1}{2}([R] - M_{s+1}),$$

$$\left| S - \frac{1}{2}(R-Q) \right| < s\frac{k+3}{2} + \frac{\tau+1}{2}.$$

Длина интервала, для которого $\frac{a}{m} - \frac{1}{m\tau} \leqslant f'(x) \leqslant \frac{a}{m} + \frac{1}{m\tau}$, не превосходит $\frac{2A}{m\tau}$. Следовательно, с одной и той же дробью $\frac{a}{m}$ связано $\leqslant \frac{2A}{m^2\tau} + 1$ чисел $m_1, m_2, \ldots, m_s$. Пусть a_1 и a_2 — наименьшее и наибольшее значения a, отвечающие данному m.

Имеем

$$\frac{a_2 - a_1}{m} - \frac{2}{m\tau} \leqslant \frac{k(R-Q)}{A}; \quad a_2 - a_1 + 1 \leqslant \frac{k(R-Q)m}{A} + 1{,}05.$$

Следовательно, с данным m связано

$$< \left(\frac{2A}{m^2\tau} + 1\right)\left(\frac{k(R-Q)m}{A} + 1{,}05\right) = \frac{k(R-Q)}{\tau}\left(\frac{2}{m} + \frac{m}{\tau^2}\right) + \left(\frac{2A}{m^2\tau} + 1\right) 1{,}05$$

чисел $m_1, m_2, \ldots, m_s$. Суммируя последнее выражение по всем $m = 1, 2, \ldots, [\tau]$, получим

$$s < \frac{k(R-Q)}{\tau}\left(2\ln\tau + 2 + \frac{\tau^2 + \tau}{2\tau^2}\right) + \frac{10A}{3\tau} 1{,}05 < \frac{k(R-Q)}{\tau} \ln A + \frac{7}{2}\frac{A}{\tau},$$

$$\left| S - \frac{1}{2}(R-Q) \right| < 2\frac{k^2(R-Q)}{\tau} \ln A + 8k\frac{A}{\tau}.$$

b. Имеем

$$\left| \sum_{Q < x \leqslant R} (f(x) + 1 - \sigma) - \frac{1}{2}(R-Q) \right| < \lambda,$$

$$\left| \sum_{Q < x \leqslant R} (f(x)) - \frac{1}{2}(R-Q) \right| < \lambda,$$

откуда, полагая $\delta(x) = (f(x) + 1 - \sigma) - (f(x))$, находим

$$\left| \sum_{Q < x \leqslant R} \delta(x) \right| < 2\lambda.$$

Но при $(f(x)) < \sigma$ имеем $\delta(x) = 1 - \sigma$, а при $(f(x)) \geqslant \sigma$ имеем $\delta(x) = -\sigma$. Поэтому $|(1-\sigma)\psi(\sigma) - \sigma(R - Q - \psi(\sigma))| < 2\lambda$, откуда и получим указанную формулу.

6, a. Применим формулу вопроса 1, c, гл. II. Полагая $f(x) = \sqrt{r^2 - x^2}$, в интервале $0 \leqslant x \leqslant \frac{r}{\sqrt{2}}$ имеем

$$f'(x) = -\frac{x}{\sqrt{r^2 - x^2}}, \quad f''(x) = \frac{-r^2}{(r^2 - x^2)^{3/2}}, \quad \frac{1}{r} \leqslant |f''(x)| \leqslant \frac{\sqrt{8}}{r}.$$

Поэтому (вопрос 8, a, гл. II, вопрос 5, a)

$$T = 4r + 8\int_0^{\frac{r}{\sqrt{2}}} \sqrt{r^2 - x^2}\, dx + 8\rho\left(\frac{r}{\sqrt{2}}\right)\frac{r}{\sqrt{2}} - 8\rho(0)\cdot r - 4\frac{r}{\sqrt{2}} - 4\frac{r^2}{2} + 8\frac{r}{\sqrt{2}}\left\{\frac{r}{\sqrt{2}}\right\} + O(r^{\frac{2}{3}}\ln r) = \pi r^2 + O(r^{\frac{2}{3}}\ln r).$$

b. Имеем (вопросы 11, d и 1, d, гл. II)

$$\tau(1) + \tau(2) + \ldots + \tau(n) = 2\sum_{0 < x \leqslant \sqrt{n}} \left[\frac{n}{x}\right] - [\sqrt{n}]^2.$$

Достаточно рассмотреть лишь случай $n > 64$. Интервал $X < x \leqslant \sqrt{n}$, где $X = 2n^{\frac{1}{3}}$, разобьём на $O(\ln n)$ интервалов вида $M < x \leqslant M'$, где $M' \leqslant 2M$. Полагая $f(x) = \frac{n}{x}$, в интервале $M < x \leqslant M'$ имеем

$$f'(x) = -\frac{n}{x^2}, \quad f''(x) = \frac{2n}{x^3}; \quad \frac{n}{4M^3} \leqslant f''(x) \leqslant \frac{8n}{4M^3}.$$

Поэтому (вопрос 5, a)

$$\sum_{M<x\leqslant M'}\left\{\frac{n}{x}\right\}=\frac{1}{2}(M'-M)+O(n^{\frac{1}{3}}\ln n),$$

$$\sum_{0<x\leqslant\sqrt{n}}\left\{\frac{n}{x}\right\}=\frac{1}{2}\sqrt{n}+O(n^{\frac{1}{3}}(\ln n)^2).$$

Далее (вопрос 8, b, гл. II)

$$\sum_{0<x\leqslant\sqrt{n}}\frac{n}{x}=En+\frac{1}{2}n\ln n+\varrho(\sqrt{n})\sqrt{n}+O(1).$$

Поэтому

$$\tau(1)+\tau(2)+\ldots+\tau(n)=2En+n\ln n+2\varrho(\sqrt{n})\sqrt{n}-\sqrt{n}-n+$$
$$+2\sqrt{n}\{\sqrt{n}\}+O(n^{\frac{1}{3}}(\ln n)^2)=n(\ln n+2E-1)+O(n^{\frac{1}{3}}(\ln n)^2).$$

7. Пусть система неправильная и s — наибольшее целое с условием, что 2^s входит в нечётное число чисел системы. Одно из последних чисел мы заменим меньшим, содержащим лишь степени 2^s, входящие в нечётное число чисел оставшейся системы.

Пусть система — правильная. Число, меньшее одного из чисел T этой системы, отличается от T, по крайней мере, одним знаком в системе исчисления с основанием 2.

8, a. Добавив к каждому из чисел, представляемых указанным способом, число $H=3^n+3^{n-1}+\ldots+3+1$, получим числа, которые можно получить, заставляя в той же форме $x_n, x_{n-1}, \ldots, x_1, x_0$ пробегать значения 0, 1, 2, т. е. получим все числа $0, 1, \ldots, 2H$.

b. Указанным способом получим $m_1m_2\ldots m_k$ чисел, не сравнимых между собою по модулю $m_1m_2\ldots m_k$, так как из

$$x_1+m_1x_2+m_1m_2x_3+\ldots+m_1m_2\ldots m_{k-1}x_k\equiv$$
$$\equiv x_1'+m_1x_2'+m_1m_2x_3'+\ldots+m_1m_2\ldots m_{k-1}x_k'\pmod{m_1m_2\ldots m_k}$$

последовательно находим:

$$x_1\equiv x_1'\pmod{m_1},\quad x_1=x_1';\quad m_1x_2\equiv m_1x_2'\pmod{m_1m_2},\quad x_2=x_2';$$
$$m_1m_2x_3\equiv m_1m_2x_3'\pmod{m_1m_2m_3},\quad x_3=x_3',$$

и т. д.

9, a. Указанным способом получим $m_1m_2\ldots m_k$ чисел, не сравнимых по модулю $m_1m_2\ldots m_k$, так как из

$$M_1x_1+M_2x_2+\ldots+M_kx_k\equiv$$
$$\equiv M_1x_1'+M_2x_2'+\ldots+M_kx_k'\pmod{m_1m_2\ldots m_k}$$

следовало бы (всякое M_j, отличное от M_s, кратно m_s)

$$M_sx_s\equiv M_sx_s'\pmod{m_s},\quad x_s\equiv x_s'\pmod{m_s},\quad x_s=x_s'.$$

b. Указанным способом получим $\varphi(m_1)\varphi(m_2)\ldots\varphi(m_k)=\varphi(m_1m_2\ldots m_k)$ чисел ввиду теоремы вопроса a, не сравнимых по модулю $m_1m_2\ldots m_k$, и ввиду $(M_1x_1+M_2x_2+\ldots+M_kx_k, m_s)=(M_sx_s, m_s)=1$, взаимно простых с $m_1m_2\ldots m_k$.

c. Согласно теореме вопроса a число $M_1x_1+M_2x_2+\ldots+M_kx_k$, где $x_1, x_2, \ldots, x_k$ пробегают полные системы вычетов по модулям $m_1, m_2, \ldots, m_k$, пробегает полную систему вычетов по модулю $m_1m_2\ldots m_k$. Это число взаимно просто с $m_1m_2\ldots m_k$ тогда и только тогда, когда $(x_1, m_1)=(x_2, m_2)=\ldots=(x_k, m_k)=1$. Поэтому $\varphi(m_1m_2\ldots m_k)=\varphi(m_1)\varphi(m_2)\ldots\varphi(m_k)$.

d. Чтобы получить все числа ряда $1, 2, \ldots, p^\alpha$, взаимно простые с p^α, следует вычеркнуть числа этого ряда, кратные p, т. е. числа $p, 2p, \ldots, p^{\alpha-1}p$. Поэтому $\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}$. Отсюда и из теоремы c, § 4, гл. II известное выражение для $\varphi(a)$ следует непосредственно.

10, a. Первое утверждение следует из

$$\left\{\frac{x_1}{m_1}+\ldots+\frac{x_k}{m_k}\right\}=\left\{\frac{M_1x_1+\ldots+M_kx_k}{m}\right\};$$

второе утверждение следует из

$$\left\{\frac{\xi_1}{m_1}+\ldots+\frac{\xi_k}{m_k}\right\}=\left\{\frac{M_1\xi_1+\ldots+M_k\xi_k}{m}\right\}.$$

b. Дроби $\left\{\frac{f_1(x_1,\ldots,w_1)}{m_1}+\ldots+\frac{f_k(x_k,\ldots,w_k)}{m_k}\right\}$ совпадают с дробями

$$\left\{\frac{f_1(M_1x_1+\ldots+M_kx_k,\ldots,M_1w_1+\ldots+M_kw_k)}{m_1}+\ldots+\right.$$
$$\left.+\frac{f_k(M_1x_1+\ldots+M_kx_k,\ldots,M_1w_1+\ldots+M_kw_k)}{m_k}\right\},$$

т. е. с дробями $\left\{\frac{f_1(x,\ldots,w)}{m_1}+\ldots+\frac{f_k(x,\ldots,w)}{m_k}\right\}$. Отсюда тривиально получается первое утверждение. Второе утверждение доказывается аналогичным способом.

11, a. При a, кратном m, имеем

$$\sum_x e^{2\pi i\frac{ax}{m}}=\sum_x 1=m.$$

При a, не делящемся на m, имеем

$$\sum_x e^{2\pi i \frac{ax}{m}} = \frac{e^{2\pi i \frac{am}{m}} - 1}{e^{2\pi i \frac{a}{m}} - 1} = 0.$$

b. При нецелом α левая часть равна

$$\left| \frac{e^{2\pi i\alpha(M+P)} - e^{2\pi i\alpha M}}{e^{2\pi i\alpha} - 1} \right| \leqslant \frac{1}{\sin \pi(\alpha)} \leqslant \frac{1}{h(\alpha)}.$$

c. Согласно теореме вопроса b левая часть не превосходит T_m, где

$$T_m = \sum_{a=1}^{m-1} \frac{1}{h\left(\frac{a}{m}\right)}.$$

Но при нечётном m

$$T_m < m \sum_{0<a<\frac{m}{2}} \ln \frac{2a+1}{2a-1} = m \ln m,$$

а при чётном m

$$T_m < \frac{m}{2} \sum_{0<a\leqslant\frac{m}{2}} \ln \frac{2a+1}{2a-1} + \frac{m}{2} \sum_{0<a<\frac{m}{2}} \ln \frac{2a+1}{2a-1} < m \ln m.$$

При $m \geqslant 6$ ввиду $\frac{1}{2} - \frac{1}{3} = \frac{1}{6}$ границу $m \ln m$ можно уменьшить на

$$2\frac{m}{6} \sum_{0<a\leqslant\frac{m}{6}} \ln \frac{2a+1}{2a-1} = \frac{m}{3} \ln\left(2\left[\frac{m}{6}\right]+1\right).$$

Последнее выражение $> \frac{m}{2}$ при $m \geqslant 12$ и $> m$ при $m \geqslant 60$.

12, a. Пусть $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ — каноническое разложение числа m. Полагая $p_1^{\alpha_1} = m_1, \dots, p_k^{\alpha_k} = m_k$, при обозначениях вопроса 10, a, имеем

$$\sum_{\xi_1} e^{2\pi i \frac{\xi_1}{m_1}} \dots \sum_{\xi_k} e^{2\pi i \frac{\xi_k}{m_k}} = \sum_{\xi} e^{2\pi i \frac{\xi}{m}}.$$

Но при $\alpha_s = 1$ находим

$$\sum_{\xi_s} e^{2\pi i \frac{\xi_s}{m_s}} = \sum_{x_s} e^{2\pi i \frac{x_s}{m_s}} - 1 = -1.$$

При $\alpha_s > 1$, полагая $m_s = p_s m_s'$, находим

$$\sum_{\xi_s} e^{2\pi i \frac{\xi_s}{m_s}} = \sum_{x_s} e^{2\pi i \frac{x_s}{m_s}} - \sum_{u=0}^{m_s'-1} e^{2\pi i \frac{u}{m_s'}} = 0.$$

b. Пусть m — целое, $m > 1$. Имеем $\sum_{x=0}^{m-1} e^{2\pi i \frac{x}{m}} = 0$. Сумма слагаемых левой части этого равенства с условием $(x, m) = d$ согласно теореме вопроса a равна $\mu\left(\frac{m}{d}\right)$.

c. Находим

$$\sum_{\xi} e^{2\pi i \frac{\xi}{m}} = \sum_{d \backslash m} \mu(d) S_d,$$

где, полагая $m = m_3 d$, имеем

$$S_d = \sum_{u=0}^{m_3-1} e^{2\pi i \frac{u}{m_3}}.$$

Последнее равно 0 при $d < m$ и равно 1 при $d = m$. Отсюда и получаем теорему вопроса a.

d. Равенства следуют из вопроса 10, b.

e. Имеем

$$A(m_1) \dots A(m_k) = m^{-r} \sum_{a_1} \dots \sum_{a_k} S_{a_1, m_1} \dots S_{a_k, m_k},$$

где $a_1, \dots, a_k$ пробегают приведённые системы вычетов по модулям $m_1, \dots, m_k$. Отсюда (вопрос d) первое равенство вопроса следует непосредственно.

Аналогичным путём докажем и второе равенство.

13, a. Имеем

$$\sum_{x=0}^{p-1} e^{2\pi i \frac{nx}{p}} = \begin{cases} p, & \text{если } n \text{ кратно } p, \\ 0 & \text{в противном случае.} \end{cases}$$

b. Раскрывая произведение, отвечающее данному n, имеем

$$\sum_{d \setminus a} \frac{\mu(d)}{d} \sum_{x=0}^{d-1} e^{2\pi i \frac{nx}{d}}.$$

Отсюда, суммируя по всем $n = 0, 1, \ldots, a-1$, и получим известное выражение для $\varphi(a)$.

14. Часть выражения, стоящего справа, отвечающая x, делящему a, равна

$$\lim_{s \to 0} 2s \sum_{k=1}^{\infty} \frac{1}{k^{1+s}} = \lim_{s \to 0} \left(2s \left(\int_1^{\infty} \frac{dx}{x^{1+s}} + O(1) \right) \right) = 2.$$

Полагая $\Phi(K) = \sum_{k=1}^{K} e^{2\pi i \frac{ak}{x}}$, часть, отвечающую x, не делящему a, можно представить в форме

$$\lim_{s \to 0} 2s \left(\frac{\Phi(1)}{1} + \frac{\Phi(2) - \Phi(1)}{2^{1+s}} + \frac{\Phi(3) - \Phi(2)}{3^{1+s}} + \ldots \right) =$$

$$= \lim_{s \to 0} 2s \left(\Phi(1) \left(1 - \frac{1}{2^{1+s}} \right) + \Phi(2) \left(\frac{1}{2^{1+s}} - \frac{1}{3^{1+s}} \right) + \ldots \right).$$

Множитель, стоящий при $2s$ ввиду $|\Phi(K)| < x$ численно $< x$; при этом $\lim_{s \to 0} 2sx = 0$. Поэтому правая часть равенства, указанного в вопросе, равна удвоенному числу делителей числа a, меньших $\frac{1}{2}a$, сложенному с δ, т. е. равна $\tau(a)$.

15, a. Имеем

$$(h_1 + h_2)^p =$$

$$= h_1^p + \binom{p}{1} h_1^{p-1} h_2 + \ldots + \binom{p}{p-1} h_1 h_2^{p-1} + h_2^p \equiv h_1^p + h_2^p \pmod{p};$$

$$(h_1 + h_2 + h_3)^p \equiv (h_1 + h_2)^p + h_3^p \equiv h_1^p + h_2^p + h_3^p \pmod{p},$$

и т. д.

b. Полагая $h_1 = h_2 = \ldots = h_a = 1$, из теоремы вопроса a получим теорему Ферма.

c. Пусть $(a, p) = 1$. При некоторых целых $N_1, N_2, \ldots, N_a$ имеем

$$a^{(p-1)} = 1 + N_1 p, \quad a^{p(p-1)} = (1 + N_1 p)^p = 1 + N_2 p^2,$$

$$a^{p^2(p-1)} = 1 + N_3 p^3, \ldots, a^{p^{\alpha-1}(p-1)} = 1 + N_\alpha p^\alpha,$$

$$a^{\varphi(p^\alpha)} \equiv 1 \pmod{p^\alpha}.$$

Пусть $m = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ — каноническое разложение числа m. Имеем

$$a^{\varphi(p_1^{\alpha_1})} \equiv 1 \pmod{p_1^{\alpha_1}}, \ldots, a^{\varphi(p_k^{\alpha_k})} \equiv 1 \pmod{p_k^{\alpha_k}},$$

$$a^{\varphi(m)} \equiv 1 \pmod{p_1^{\alpha_1}}, \ldots, a^{\varphi(m)} \equiv 1 \pmod{p_k^{\alpha_k}},$$

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Решения к главе IV.

1, a. Теорема непосредственно следует из теоремы вопроса 11, a, гл. III.

b. Пусть d — делитель числа m, $m = m_0 d$, H_d обозначает сумму слагаемых с условием $(a, m) = d$ в выражении для Tm вопроса a. Находим

$$H_d = \sum_{a_0} \sum_{x=0}^{m-1} \cdots \sum_{w=0}^{m-1} e^{2\pi i \frac{a_0 f(x, \ldots, w)}{m_0}},$$

где a_0 пробегает приведённую систему вычетов по модулю m_0. Отсюда выводим

$$H_d = d^r \sum_{a_0} \sum_{x_0=0}^{m_0-1} \cdots \sum_{w_0=0}^{m_0-1} e^{2\pi i \frac{a_0 f(x_0, \ldots, w_0)}{m_0}} = m^r A(m_0).$$

c. Пусть $m > 0$, $(a, m) = d$, $a = a_0 d$, $m = m_0 d$, T — число решений сравнения $ax \equiv b \pmod{m}$. Имеем

$$Tm = \sum_{s=0}^{m-1} \sum_{x=0}^{m-1} e^{2\pi i \frac{s(ax-b)}{m}} =$$

$$= \sum_{s=0}^{m-1} \sum_{x=0}^{m-1} e^{2\pi i \frac{sa_0}{m_0} x - 2\pi i \frac{bs}{m}} =$$

$$= m \sum_{s_1=0}^{d-1} e^{-2\pi i \frac{bs_1}{d}} = \begin{cases} md, & \text{если } b \text{ кратно } a, \\ 0 & \text{в противном случае.} \end{cases}$$

d. Полагая $(a, m)=d_1$, $(b, d_1)=d_2, \ldots, (f, d_{r-1})=d_r$, $m=d_1m_1$, $d_1=d_2m_2, \ldots, d_{r-1}=d_rm_r$, находим $d=d_r$,

$$Tm=\sum_{u=0}^{m-1}\sum_{x=0}^{m-1}\sum_{y=0}^{m-1}\cdots\sum_{w=0}^{m-1}e^{2\pi i\frac{u(ax+by+\ldots+fw+g)}{m}}=$$

$$=m\sum_{\alpha_1=0}^{d_1-1}\sum_{y=0}^{m-1}\cdots\sum_{w=0}^{m-1}e^{2\pi i\frac{\alpha_1(by+\ldots+fw+g)}{d_1}}=$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$=m^{r-1}\sum_{\alpha_{r-1}=0}^{d_{r-1}-1}\sum_{w=0}^{m-1}e^{2\pi i\frac{\alpha_{r-1}(fw+g)}{d_{r-1}}}=m^r\sum_{\alpha_r=0}^{d_r-1}e^{2\pi i\frac{\alpha_r g}{d_r}}.$$

e. Применим метод индукции. Пусть при обозначениях вопроса d теорема верна для r переменных. Рассмотрим сравнение

$$lv+ax+\ldots+fw+g\equiv 0\pmod m. \qquad (2)$$

Пусть $(l, m)=d_0$. Условием возможности сравнения (2) будет $ax+\ldots+fw+g\equiv 0\pmod{d_0}$. Последнее сравнение возможно лишь в случае, когда g кратно d', где $d'=(a, \ldots, f, d_0)=(l, a, \ldots, f, m)$, причём тогда оно имеет $d_0^{r-1}d'$ решений. Следовательно, сравнение (2) возможно лишь в случае, когда g кратно d', и тогда оно имеет $d_0^{r-1}d'\left(\frac{m}{d_0}\right)^r d_0=m^r d'$ решений. Таким образом теорема верна и для $r+1$ переменных. Но теорема верна для одного переменного. Значит, она верна всегда.

2, a. Имеем $a^{\varphi(m)}\equiv 1\pmod m$, $a\cdot ba^{\varphi(m)-1}\equiv b\pmod m$.

b. Имеем

$$1\cdot 2\ldots(a-1)ab(-1)^{a-1}\frac{(p-1)\ldots(p-a+1)}{1\cdot 2\ldots a}\equiv$$
$$\equiv b\cdot 1\cdot 2\ldots(a-1)\pmod p,$$

откуда, деля почленно на $1\cdot 2\ldots(a-1)$, и получим указанную теорему.

c. α) Достаточно, очевидно, ограничиться случаем $(2, b)=1$. Выбирая надлежащим образом знак, имеем $b\pm m\equiv 0\pmod 4$. Пусть 2^δ — наибольшая степень 2, делящая $b\pm m$. При $\delta\geqslant k$ имеем

$$x\equiv\frac{b\pm m}{2^k}\pmod m.$$

Если же $\delta<k$, то имеем

$$2^{k-\delta}x\equiv\frac{b\pm m}{2^\delta}\pmod m.$$

С этим сравнением повторяем аналогичную операцию, и т. д.

β) Считаем $(3, b)=1$. Выбрав надлежащим образом знак, имеем $b\pm m\equiv 0\pmod 3$. Пусть 3^δ — наибольшая степень 3, делящая $b\pm m$. При $\delta\geqslant k$ имеем

$$x\equiv\frac{b\pm m}{3^k}\pmod m$$

Если же $\delta<k$, то имеем

$$3^{k-\delta}x\equiv\frac{b\pm m}{3^\delta}\pmod m.$$

С этим сравнением повторяем аналогичную операцию, и т. д.

γ) Пусть p — простой делитель числа a. Найдём t из условия $b+mt\equiv 0\pmod p$. Пусть p^δ — наибольшая степень p, делящая $(a, b+mt)$, и пусть $a=a_1p^\delta$. Имеем

$$a_1x\equiv\frac{b+mt}{p^\delta}\pmod m$$

Если $a_1>1$, то с этим новым сравнением повторяем аналогичную операцию, и т. д.

Указанный способ удобен в случае небольших простых сомножителей числа a.

3. Полагая $\tau=[\tau]$, пишем сравнения

$$a\cdot 0\equiv 0\pmod m,$$
$$a\cdot 1\equiv y_1\pmod m,$$
$$\cdots\cdots\cdots$$
$$a\cdot t\equiv y_t\pmod m,$$
$$a\cdot 0\equiv m\pmod m.$$

Расположив эти сравнения в порядке возрастания правых частей (ср. вопрос 4, a, гл. II) и вычитая почленно каждое сравнение (кроме последнего) из следующего за ним, получим $t+1$ сравнений вида $ax\equiv u\pmod m$: $0<|x|\leqslant\tau$. При этом, по крайней мере, в одном сравнении будет $0<u<\frac{m}{\tau}$. Действительно, u имеет $t+1>\tau$ значений, эти значения положительные, и их сумма равна m.

4, a, α) Следует из определения символической дроби.

β) Здесь можно положить $b_0=b+mt$, где t определяется из условия $b+mt\equiv 0\pmod a$; тогда сравнению $ax\equiv b$ удовлетворит целое число, представляемое обычной дробью $\frac{b_0}{a}$.

γ) Имеем (b_0 кратно a, d_0 кратно c)

$$\frac{b}{a}+\frac{d}{c}\equiv\frac{b_0}{a}+\frac{d_0}{c}=\frac{b_0c+ad_0}{ac}\equiv\frac{bc+ad}{ac}.$$

δ) Имеем

$$\frac{b}{a}\cdot\frac{d}{c}\equiv\frac{b_0}{a}\cdot\frac{d_0}{c}=\frac{b_0d_0}{ac}\equiv\frac{bd}{ac}.$$

b, α) Имеем (сравнения берутся по модулю p)

$$\binom{p-1}{a}=\frac{(p-1)(p-2)\dots(p-a)}{1\cdot2\dots a}\equiv\frac{(-1)^a1\cdot2\dots a}{1\cdot2\dots a}\equiv(-1)^a.$$

Вопрос 2, b теперь проще решать так:

$$\frac{b}{a}\equiv\frac{b(-1)^{a-1}(p-1)\dots(p-(a-1))}{1\cdot2\dots(a-1)a}\pmod p$$

β) Имеем

$$\frac{2^p-2}{p}\equiv1+\frac{p-1}{1\cdot2}+\frac{(p-1)(p-2)}{1\cdot2\cdot3}+\dots+\frac{(p-1)(p-2)\dots(p-(p-2))}{1\cdot2\dots(p-1)}\pmod p.$$

5, a. Числа s, $s+1$, …, $s+n-1$ попарно не могут иметь общих делителей с d. Произведения $s(s+1)\dots(s+n-1)$ могут быть объединены в n^k совокупностей по числу способов, сколькими число d может быть разбито на n попарно простых сомножителей с учётом порядка последних (вопрос 11, b, гл. II). Пусть $d=u_1u_2\dots u_n$ — одно из таких разбиений. Число произведений с условием $s\equiv0\pmod{u_1}$, $s+1\equiv0\pmod{u_2}$,…, $s+n-1\equiv0\pmod{u_n}$ равно $\frac{a}{d}$. Поэтому искомое число равно $n^k\frac{a}{d}$.

b. Указанное число равно

$$\sum_{d\setminus a}\mu(d)S_d;\quad S_d=\frac{n^k a}{d},$$

где k — число различных простых делителей числа d. Но имеем

$$\sum_{d\setminus a}\mu(d)\frac{n^k a}{d}=a\left(1-\frac{n}{p_1}\right)\left(1-\frac{n}{p_2}\right)\dots\left(1-\frac{n}{p_k}\right).$$

6, a. Все значения x, удовлетворяющие первому сравнению, даются равенством $x=b_1+m_1t$, где t — целое. Чтобы выбрать из них те, которые удовлетворяют также и второму сравнению, надо ограничиться лишь теми значениями t, которые удовлетворяют сравнению

$$m_1t\equiv b_2-b_1\pmod{m_2}.$$

Но это сравнение разрешимо тогда и только тогда, когда b_2-b_1 кратно d. При этом в случае разрешимости совокупность значений t, ему удовлетворяющих, определяется равенством вида $t=t_0+\frac{m_2}{d}t'$, где t' — целое; вместе с тем совокупность значений x, удовлетворяющих рассматриваемой в вопросе системе, определится равенством

$$x=b_1+m_1\left(t_0+\frac{m_2}{d}t'\right)=x_{1,2}+m_{1,2}t';\ x_{1,2}=b_1+m_1t_0.$$

b. В случае разрешимости системы

$$x\equiv b_1\pmod{m_1},\quad x\equiv b_2\pmod{m_2}$$

совокупность значений x, ей удовлетворяющих, представится сравнением вида $x\equiv x_{1,2}\pmod{m_{1,2}}$. В случае разрешимости системы

$$x\equiv x_{1,2}\pmod{m_{1,2}},\quad x\equiv b_3\pmod{m_3}$$

совокупность значений x, ей удовлетворяющих, представится сравнением вида $x\equiv x_{1,2,3}\pmod{m_{1,2,3}}$. В случае разрешимости системы

$$x\equiv x_{1,2,3}\pmod{m_{1,2,3}},\quad x\equiv b_4\pmod{m_4}$$

совокупность значений x, ей удовлетворяющих, представится сравнением вида $x\equiv x_{1,2,3,4}\pmod{m_{1,2,3,4}}$, и т. д.

7, α) От замены x на $-x$ (вследствие чего x' заменится на $-x'$) величина суммы $\left(\frac{a,b}{m}\right)$ не изменится.

β) Когда x пробегает приведённую систему вычетов по модулю m, то и x' пробегает приведённую систему вычетов по модулю m.

γ) Полагая $x\equiv hz\pmod m$, получим

$$\left(\frac{a,bh}{m}\right)=\sum_z e^{2\pi i\frac{ahz+bz'}{m}}=\left(\frac{ah,b}{m}\right).$$

δ) Имеем

$$\left(\frac{a_1,\ 1}{m_1}\right)\left(\frac{a_2,\ 1}{m_2}\right)=\sum_x\sum_y e^{2\pi i\frac{a_1m_2x+a_2m_1y+m_2x'+m_1y'}{m_1m_2}}.$$

Полагая $m_2x'+m_1y'=z'$, имеем

$$(a_1m_2x+a_2m_1y)(m_2x'+m_1y')\equiv a_1m_2^2+a_2m_1^2\pmod{m_1m_2},$$

$$\left(\frac{a_1,\ 1}{m_1}\right)\left(\frac{a_2,\ 1}{m_2}\right)=\left(\frac{m_2^2a_1+m_1^2a_2,\ 1}{m_1m_2}\right),$$

что и доказывает указанное свойство в случае двух сомножителей. Обобщение на случай более чем двух сомножителей тривиально.

8. Сравнение

$$a_0x^n + a_1x^{n-1} + \ldots + a_n - a_0(x-x_1)(x-x_2)\ldots(x-x_n) \equiv 0 \pmod p$$

имеет n решений. Оно степени ниже n. Следовательно, все его коэффициенты кратны p, а это и выражается сравнениями, указанными в вопросе.

9, a. При $p > 3$ соответственно x, взятому из ряда 2, 3, ..., $p-2$, найдём отличное от него число x' того же ряда с условием $xx' \equiv 1 \pmod p$; действительно, из $x = x'$ следовало бы $(x-1)(x+1) \equiv 0 \pmod p$; $x \equiv 1$ или $x \equiv p-1$. Поэтому

$$2\cdot 3\ldots(p-2) \equiv 1 \pmod p; \quad 1\cdot 2\ldots(p-1) \equiv -1 \pmod p.$$

b. Пусть $P > 2$. Допустив, что P имеет делитель u с условием $1 < u < P$, мы имели бы $1\cdot 2\ldots(P-1)+1 \equiv 1 \pmod u$.

10, a. Находим h с условием $a_0h \equiv 1 \pmod m$. Данное сравнение равносильно такому:

$$x^n + a_1hx^{n-1} + \ldots + a_nh \equiv 0 \pmod m.$$

b. Пусть $Q(x)$ — частное и $R(x)$ — остаток от деления $x^p - x$ на $f(x)$. Все коэффициенты $Q(x)$ и $R(x)$ — целые, $Q(x)$ — степени $p-n$, $R(x)$ — степени ниже n,

$$x^p - x = f(x)\,Q(x) + R(x).$$

Пусть сравнение $f(x) \equiv 0 \pmod p$ имеет n решений. Те же решения будут решениями и сравнения $R(x) \equiv 0 \pmod p$; поэтому все коэффициенты $R(x)$ кратны p.

Обратно, пусть все коэффициенты $R(x)$ кратны p. Тогда $f(x)\,Q(x)$ кратно p при тех же значениях x, что и $x^p - x$; поэтому сумма чисел решений сравнений

$$f(x) \equiv 0 \pmod p, \quad Q(x) \equiv 0 \pmod p$$

не меньше чем p. Пусть первое имеет α, а второе β решений. Из

$$\alpha \leqslant n, \ \beta \leqslant p-n, \ p \leqslant \alpha + \beta$$

выводим $\alpha = n$, $\beta = p-n$.

c. Возвышая данное сравнение почленно в степень $\frac{p-1}{n}$, убеждаемся в необходимости указанного условия. Пусть это условие выполнено; из $x^p - x = x(x^{p-1} - A^{\frac{p-1}{n}} + A^{\frac{p-1}{n}} - 1)$ следует, что остаток от деления $x^p - x$ на $x^n - A$ есть $(A^{\frac{p-1}{n}} - 1)x$, где $A^{\frac{p-1}{n}} - 1$ кратно p.

11. Из $x_0^n \equiv A \pmod m$, $y^n \equiv 1 \pmod m$ следует $(x_0y)^n \equiv A \pmod m$; при этом произведения x_0y, отвечающие несравнимым (по модулю m) y, несравнимы. Из $x_0^n \equiv A \pmod m$, $x^n \equiv A \pmod m$ следует $x^n \equiv x_0^n \pmod m$, причём, определяя y условием $x \equiv yx_0 \pmod m$, имеем

$$y^n \equiv 1 \pmod m.$$

Решения к главе V.

1. Указанное сравнение равносильно такому: $(2ax+b)^2 \equiv b^2 - 4ac \pmod m$. Соответственно каждому решению $z \equiv z_0 \pmod m$ сравнения $z^2 \equiv b^2 - 4ac \pmod m$ из $2ax + b \equiv z_0 \pmod m$ найдём одно решение указанного сравнения.

2, a. При $\left(\frac{a}{p}\right) = 1$ имеем $a^{2m+1} \equiv 1 \pmod p$, $(a^{m+1})^2 \equiv a \pmod p$, $x \equiv \pm a^{m+1} \pmod p$.

b. При $\left(\frac{a}{p}\right) = 1$ имеем $a^{4m+2} \equiv 1 \pmod p$, $a^{2m+1} \equiv \pm 1 \pmod p$, $a^{2m+2} \equiv \pm a \pmod p$.

Ввиду $\left(\frac{2}{p}\right) = -1$ имеем также $2^{4m+2} \equiv -1 \pmod p$. Поэтому при некотором s, имеющем одно из значений 0; 1, получим

$$a^{2m+2}2^{(4m+2)s} \equiv a \pmod p, \quad x \equiv \pm a^{m+1}2^{(2m+1)s} \pmod p.$$

c. Пусть $p = 2^kh + 1$, где $k \geqslant 3$ и h — нечётное, $\left(\frac{a}{p}\right) = 1$. Имеем

$$a^{2^{k-1}h} \equiv 1 \pmod p, \quad a^{2^{k-2}h} \equiv \pm 1 \pmod p, \quad N^{2^{k-1}h} \equiv -1 \pmod p.$$

Поэтому при некотором целом неотрицательном s_2 получим

$$a^{2^{k-2}h}N^{s_2}2^{k-1} \equiv 1 \pmod p, \quad a^{2^{k-3}h}N^{s_2}2^{k-2} \equiv \pm 1 \pmod p;$$

отсюда при некотором целом неотрицательном s_3 получим

$$a^{2^{k-3}h}N^{s_3}2^{k-2} \equiv 1 \pmod p, \quad a^{2^{k-4}h}N^{s_3}2^{k-3} \equiv \pm 1 \pmod p,$$

и т. д.; наконец, получим

$$a^hN^{s_k} \equiv 1 \pmod p, \quad x \equiv \pm a^{\frac{h+1}{2}}N^{s_k} \pmod p.$$

d. Имеем

$$1\cdot 2\ldots 2m\,(p-2m)\ldots(p-2)(p-1)+1 \equiv 0 \pmod p,$$
$$(1\cdot 2\ldots 2m)^2 + 1 \equiv 0 \pmod p.$$

3, a. Условия разрешимости сравнений (1) и (2) выводятся тривиально (f, § 2 и k, § 2). Сравнение (3) разрешимо тогда и только

тогда, когда $\left(\frac{-3}{p}\right)=1$. Но $\left(\frac{-3}{p}\right)=\left(\frac{p}{3}\right)$, причём

$$\left(\frac{p}{3}\right)=\begin{cases} 1, & \text{если } p \text{ имеет вид } 6m+1,\\ -1, & \text{если } p \text{ имеет вид } 6m+5.\end{cases}$$

b. Каковы бы ни были различные простые $p_1, p_2, \ldots, p_k$ вида $4m+1$, наименьший простой делитель p числа $(2p_1p_2\ldots p_k)^2+1$ будет отличен от $p_1, p_2, \ldots, p_k$ и ввиду $(2p_1p_2\ldots p_k)^2+1\equiv 0 \pmod p$ имеет вид $4m+1$.

c. Каковы бы ни были различные простые $p_1, p_2, \ldots, p_k$ вида $6m+1$, наименьший простой делитель p числа $(2p_1p_2\ldots p_k)^2+3$ будет отличен от $p_1, p_2, \ldots, p_k$ и ввиду $(2p_1p_2\ldots p_k)^2+3\equiv 0 \pmod p$ имеет вид $6m+1$.

4. Среди чисел первой совокупности будут числа, сравнимые с $1\cdot 1, 2\cdot 2, \ldots, \frac{p-1}{2}\frac{p-1}{2}$, т. е. все квадратичные вычеты полной системы; число, входящее по условию во вторую совокупность, будет квадратичный невычет. Но во вторую совокупность войдут все произведения этого невычета на все вычеты, т. е. войдут все квадратичные невычеты.

5, a. Пусть в системе исчисления с основанием p

$$a=a_{\alpha-1}p^{\alpha-1}+\ldots+a_1p+a_0$$

и искомое решение (наименьший неотрицательный вычет)

$$x=x_{\alpha-1}p^{\alpha-1}+\ldots+x_1p+x_0. \qquad (1)$$

Составим таблицу:

$a_{\alpha-1}$	$\ldots$	a_4	a_3	a_2	a_1	a_0
$2x_0x_{\alpha-1}$	$\ldots$	$2x_0x_4$	$2x_0x_3$	$2x_0x_2$	$2x_0x_1$	x_0^2
$2x_1x_{\alpha-2}$	$\ldots$	$2x_1x_3$	$2x_1x_2$	x_1^2		
$2x_2x_{\alpha-3}$	$\ldots$	x_2^2				
$\ldots$						

где в столбце под a_s стоят числа, сумма которых образует коэффициент при p^s в разложении квадрата правой части (1) по степеням p. Находим x_0 из условия

$$x_0^2\equiv a_0 \pmod p$$

Полагая $\frac{x_0^2-a_0}{p}=p_1$, находим x_1 из условия

$$p_1+2x_0x_1\equiv a_1 \pmod p.$$

Полагая $\frac{p_1+2x_0x_1-a_1}{p}=p_2$, находим x_2 из условия

$$p_2+2x_0x_2+x_1^2\equiv a_2 \pmod p.$$

и т. д. При данном x_0 ввиду $(x_0, p)=1$ числа $x_1, x_2, \ldots, x_{\alpha-1}$ определятся однозначно.

b. Здесь

$$a=a_{\alpha-1}2^{\alpha-1}+\ldots+a_32^3+a_22^2+a_12+a_0,$$
$$x=x_{\alpha-1}2^{\alpha-1}+\ldots+x_32^3+x_22^2+x_12+x_0,$$

и мы будем иметь следующую таблицу:

$a_{\alpha-1}$	$\ldots$	a_4	a_3	a_2	a_1	a_0
$x_0x_{\alpha-2}$	$\ldots$	x_0x_3	x_0x_2	x_0x_1		x_0^2
$x_1x_{\alpha-3}$	$\ldots$	x_1x_2		x_1^2		
$x_2x_{\alpha-4}$	$\ldots$	x_2^2				

Рассмотрим лишь случай $\alpha\geqslant 3$. Ввиду $(a, 2)=1$ необходимо $a_0=1$. Поэтому $x_0=1$. Далее необходимо $a_1=0$, и ввиду $x_0x_1+x_1^2=x_1+x_1^2\equiv 0 \pmod 2$ необходимо $a_2=0$. Для x_1 возможны два значения: 0 и 1. Числа $x_2, x_3, \ldots, x_{\alpha-2}$ определятся однозначно, а для $x_{\alpha-1}$ возможны два значения: 0 и 1. Поэтому при $\alpha\geqslant 3$ необходимо $a\equiv 1 \pmod 8$, и тогда указанное сравнение имеет 4 решения.

6. Очевидно, P и Q — целые, причём Q по модулю p сравнимо с числом, которое получим, заменяя a на z^2, для чего достаточно $\sqrt{a}$ заменить на z. Поэтому $Q\equiv 2^{\alpha-1}z^{\alpha-1} \pmod p$; следовательно, $(Q, p)=1$ и Q' действительно можно определить из сравнения $QQ'\equiv 1 \pmod{p^\alpha}$. Имеем

$$P^2-aQ^2=(z+\sqrt{a})^\alpha(z-\sqrt{a})^\alpha=(z^2-a)^\alpha\equiv 0 \pmod{p^\alpha},$$

откуда

$$(PQ')^2\equiv a(QQ')^2\equiv a \pmod{p^\alpha}.$$

7. Пусть $m=2^\alpha p_1^{\alpha_1}\ldots p_k^{\alpha_k}$ — каноническое разложение числа m. Тогда m представляется в форме $m=2^\alpha ab$, где $(a, b)=1$, 2^κ способами

Пусть $a=0$. Из $(x-1)(x+1)\equiv 0 \pmod m$ следует, что при некоторых a и b

$$x\equiv 1 \pmod a;\ x\equiv -1 \pmod b.$$

Решая эту систему, получим $x\equiv x_0 \pmod m$. Поэтому указанное сравнение имеет 2^α решений.

Пусть $\alpha=1$. При некоторых a и b

$$x\equiv 1 \pmod{2a};\quad x\equiv -1 \pmod{2b}.$$

Решая эту систему, получим $x\equiv x_0 \pmod m$. Поэтому указанное сравнение имеет 2^α решений.

Пусть $\alpha=2$. При некоторых a и b

$$x\equiv 1 \pmod{2a};\quad x\equiv -1 \pmod{2b}.$$

Решая эту систему, получим $x\equiv x_0 \pmod{\frac{m}{2}}$. Поэтому указанное сравнение имеет 2^{k+1} решений.

Пусть $\alpha\geqslant 3$. При некоторых a и b должна выполняться одна из систем

$$x\equiv 1 \pmod{2a};\qquad x\equiv -1 \pmod{2^{\alpha-1}b};$$

$$x\equiv 1 \pmod{2^{\alpha-1}a};\quad x\equiv -1 \pmod{2b}.$$

Решая одну из этих систем, получим $x\equiv x_0 \pmod{\frac{m}{2}}$. Поэтому указанное сравнение имеет 2^{k+1} решений.

8, а. Определяя x' сравнением $xx'\equiv 1 \pmod p$, имеем

$$\sum_{x=1}^{p-1}\left(\frac{x(x+k)}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{xx'\,(xx'+kx')}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{1+kx'}{p}\right).$$

Очевидно, $1+kx'$ пробегает все вычеты полной системы, кроме 1. Отсюда и следует указанная теорема.

b. Указанное равенство следует из

$$T=\frac{1}{4}\sum_{x=1}^{p-2}\left(1+\varepsilon\left(\frac{x}{p}\right)\right)\left(1+\eta\left(\frac{x+1}{p}\right)\right)=$$

$$=\frac{1}{4}\sum_{x=1}^{p-2}\left(1+\varepsilon\left(\frac{x}{p}\right)+\eta\left(\frac{x+1}{p}\right)+\varepsilon\eta\left(\frac{x(x+1)}{p}\right)\right).$$

c. Имеем

$$S^2\leqslant X\sum_{x=0}^{p-1}\sum_{u_1}\sum_{u}\left(\frac{(xy_1+k)(xy+k)}{p}\right)$$

Часть выражения, стоящего справа, отвечающая случаям $y_1=y$, не превосходит XpY. Рассмотрим часть, отвечающую паре не равных между собою значений y_1 и y, причём для определённости предположим, что $y>0$. Полагая $xy+k\equiv z \pmod p$, приведём указанную часть к виду

$$X\sum_{z=0}^{p-1}\left(\frac{z\left(\frac{y_1}{y}z+k\left(1-\frac{y_1}{y}\right)\right)}{p}\right),$$

откуда убедимся (вопрос a), что она численно $\leqslant X$. Поэтому $S^2<XpY+XY^2\leqslant 2pXY$.

d, α) Имеем

$$S=\sum_{x=0}^{p-1}\sum_{z_1=0}^{Q-1}\sum_{z=0}^{Q-1}\left(\frac{(x+z_1)(x+z)}{p}\right).$$

При $z_1=z$ суммирование по x даёт $p-1$. При z_1, не равном z, суммирование по x (вопрос a) даёт -1. Поэтому

$$S=(p-1)Q-Q(Q-1)=(p-Q)Q.$$

β) Согласно теореме вопроса α) имеем

$$T\,(Q^{0,5+0,5\lambda})^2<pQ;\quad T<pQ^{-\lambda}.$$

γ) Полагая $[\sqrt p]=Q$, применим теорему вопроса α). Допустив, что в указанном в вопросе ряде квадратичных невычетов нет, убедимся, что $|S_x|\geqslant Q-1$ при $x=M, M+1, \ldots, M+2Q-1$ и, таким образом,

$$2Q(Q-1)^2\leqslant(p-Q)Q,\quad 2(Q-1)^2\leqslant(Q+1)^2-Q,\quad Q^2-5Q<0,$$

что при $Q\geqslant 5$ невозможно.

9, а. Если m представляется в форме (1), то решение

$$z\equiv z_0 \pmod m \qquad (5)$$

сравнения $x\equiv zy \pmod m$ является также и решением сравнения (2). Мы будем говорить, что указанное представление связано с решением (5) сравнения (2).

С каждым решением (5) сравнения (2) связано не менее одного представления (1). Действительно, взяв $\tau=\sqrt m$, имеем

$$\frac{z_0}{m}=\frac{P}{Q}+\frac{\theta}{Q\sqrt m};\quad (P,Q)=1,\ 0<Q\leqslant\sqrt m,\ |\theta|<1.$$

Поэтому $z_0Q=mP+r$, где $|r|<\sqrt m$. Далее, из (2) следует, что $|r|^2+Q^2\equiv 0 \pmod m$. Отсюда и из $0<|r|^2+Q^2<2m$ находим

$$m=|r|^2+Q^2. \qquad (6)$$

При этом $(|r|, Q)=1$ ввиду

$$1=\frac{r^2+Q^2}{m}=\frac{(z_0Q-mP)\,z_0Q-rmP+Q^2}{m}\equiv -rP \pmod Q.$$

Если $|r|=r$, то ввиду $r\equiv z_0Q \pmod m$ представление (6) связано с решением (5). Если $|r|=-r$, то ввиду $z_0^2Q\equiv z_0r \pmod m$ $Q\equiv z_0|r| \pmod m$, представление $m=Q^2+|r|^2$ связано с решением (5).

С каждым решением (5) связано не более одного представления (1). Действительно, если два представления $m=x^2+y^2$ и $m=x_1^2+y_1^2$ числа m в форме (1) связаны с одним и тем же решением (5), то из $x\equiv z_0y \pmod m$, $x_1\equiv z_0y_1 \pmod m$ следует $xy_1\equiv x_1y \pmod m$. Поэтому $xy_1=x_1y$, откуда ввиду $(x,\ y)=(x_1,\ y_1)=1$ следует $x=x_1$, $y=y_1$.

b. Если m представляется в форме (3), то решение

$$z\equiv z_0 \pmod p \tag{7}$$

сравнения $x\equiv zy \pmod p$ является также и решением сравнения (4). Мы будем говорить, что указанное представление связано с решением (7) сравнения (4).

Зная решение (7) сравнения (4), найдём не менее одного представления (3). Действительно, взяв $\tau=\sqrt{p}$, имеем

$$\frac{z_0}{p}=\frac{P}{Q}+\frac{\theta}{Q\sqrt{p}};\quad (P, Q)=1,\quad 0<Q\leqslant\sqrt{p},\quad |\theta|<1.$$

Поэтому $z_0Q\equiv r \pmod p$, где $|r|<p$. Далее из (4) следует, что $|r|^2+aQ^2\equiv 0 \pmod p$. Отсюда и из $0<|r|^2+aQ^2<(1+a)\,p$ следует, что при $a=2$ должно быть или $|r|^2+2Q^2=p$, или $|r|^2+2Q^2=2p$. В последнем случае $|r|$ — чётное, $|r|=2r_1$, $p=Q^2+2r_1^2$. При $a=3$ должно быть или $|r|^2+3Q^2=p$, или $|r|^2+3Q^2=2p$, или $|r|^2+3Q^2=3p$. Второй случай невозможен: по модулю 4 левая часть сравнима с 0, а правая — с 2. В третьем случае $|r|$ кратно 3, $|r|=3r_1$, $p=Q^2+3r_1^2$.

Допустив, что два представления $p=x^2+ay^2$ и $p=x_1^2+ay_1^2$ числа p в форме (3) связаны с одним и тем же решением сравнения (4), найдём $x=x_1$, $y=y_1$. Допустив, что эти представления связаны с различными решениями сравнения (4), найдём $x\equiv zy \pmod p$, $x_1\equiv -zy_1 \pmod p$, откуда $xy_1+x_1y\equiv 0 \pmod p$, что ввиду $0<(xy_1+x_1y)^2\leqslant(x^2+y^2)\,(x_1^2+y_1^2)<p^2$ невозможно.

c. α) Слагаемые суммы $S(k)$ с $x=x_1$ и $x=-x_1$ равны между собою.

β) Имеем

$$S(kt^2)=\sum_{x=0}^{p-1}\left(\frac{xt\,(x^2t^2+kt^2)}{p}\right)=\left(\frac{t}{p}\right)S(k).$$

γ) Полагая $p-1=2p_1$, имеем

$$p_1(S(r))^2+p_1(S(n))^2=\sum_{t=1}^{p_1}(S(rt^2))^2+\sum_{t-1}^{p_1}(S(nt^2))^2=$$

$$=\sum_{k=1}^{p-1}(S(k))^2=\sum_{x=1}^{p-1}\sum_{y=1}^{p-1}\sum_{k=1}^{p-1}\left(\frac{xy\,(x^2+k)\,(y^2+k)}{p}\right).$$

При y, не равном x или $p-x$, результат суммирования по k будет $-2\left(\frac{xy}{p}\right)$; при $y=x$ или $y=p-x$ он будет $(p-2)\left(\frac{xy}{p}\right)$. Поэтому

$$p_1(S(r))^2+p_1(S(n))^2=4pp_1,\quad p=\left(\frac{1}{2}S(r)\right)^2+\left(\frac{1}{2}S(n)\right)^2.$$

10, a. Имеем

$$X^2-DY^2=(x_1+y_1\sqrt{D})\,(x_2\pm y_2\sqrt{D})\,(x_1-y_1\sqrt{D})\,(x_2\mp y_2\sqrt{D})=k^2.$$

b. Взяв любое τ_1 с условием $\tau_1>1$, найдём целые x_1, y_1 с условиями $|y_1\sqrt{D}-x_1|<\frac{1}{\tau_1}$, $0<y\leqslant\tau_1$, откуда, умножая почленно на $y_1\sqrt{D}+x_1<2y_1\sqrt{D}+1$, получим $|x_1^2-Dy_1^2|<2\sqrt{D}+1$. Взяв $\tau_2>\tau_1$ с условием $|y_1\sqrt{D}-x_1|>\frac{1}{\tau_2}$, найдём новые целые x_2, y_2 с условием $|x_2^2-Dy_2^2|<2\sqrt{D}+1$, и т. д.

Очевидно, в интервале $-2\sqrt{D}-1<k<2\sqrt{D}+1$ существует такое целое, не равное нулю k, что среди пар x_1, y_1; x_2, y_2; ... найдётся бесчисленное множество пар x, y с условием $x^2-Dy^2=k$; среди же последних наверно найдутся две пары ξ_1, η_1 и ξ_2, η_2 с условием $\xi_2\equiv\xi_1 \pmod{|k|}$, $\eta_1\equiv\eta_2 \pmod{|k|}$. Определяя целые ξ_0, η_0 равенством $\xi_0+\eta_0\sqrt{D}=(\xi_1+\eta_1\sqrt{D})\,(\xi_2-\eta_2\sqrt{D})$, имеем (вопрос a)

$$\xi_0^2-D\eta_0^2=|k|^2;\ \xi_0\equiv\xi_1^2-D\eta_1^2\equiv 0 \pmod{|k|};$$

$$\eta_0\equiv -\xi_1\eta_1+\xi_1\eta_1\equiv 0 \pmod{|k|}.$$

Поэтому $\xi_0=\xi|k|$, $\eta_0=\eta|k|$, где ξ и η — целые и $\xi^2-D\eta^2=1$.

c. Числа x, y, определяемые равенством (2), удовлетворяют (вопрос a) уравнению (1).

Допустив существование пары целых положительных x, y, удовлетворяющих уравнению (1), но отличной от пар, определяемых равенством (2), мы при некотором $r=1, 2, \ldots$ будем иметь

$$(x_0+y_0\sqrt{D})^r<x+y\sqrt{D}<(x_0+y_0\sqrt{D})^{r+1}.$$

Отсюда, деля почленно на $(x_0+y_0\sqrt{D})^r$, получим

$$1<X+Y\sqrt{D}<x_0+y_0\sqrt{D}, \tag{3}$$

где (вопрос а) X и Y — целые, определяемые равенством

$$X+Y\sqrt{D}=\frac{x+y\sqrt{D}}{(x_0+y_0\sqrt{D})^r}=(x+y\sqrt{D})(x_0-y_0\sqrt{D})^r$$

и удовлетворяющие уравнению

$$X^2-DY^2=1. \tag{4}$$

Но из (4) следуют неравенства $0<|X|-|Y\sqrt{D}|<1$, которые в соединении с первым неравенством (3) показывают, что X и Y — положительные. Поэтому второе неравенство (3) противоречит определению чисел x_0 и y_0.

11, а, α) Имеем

$$|U_{a,p}|^2=U_{a,p}\overline{U}_{a,p}=\sum_{t=1}^{p-1}\sum_{x=1}^{p-1}\left(\frac{t}{p}\right)e^{2\pi i\frac{ax(t-1)}{p}}.$$

При $t=1$ суммирование по x даёт $p-1$; при $t>1$ оно даёт $-\left(\frac{t}{p}\right)$. Поэтому

$$|U_{a,p}|^2=p-1-\sum_{t=2}^{p-1}\left(\frac{t}{p}\right)=p,\ |U_{a,p}|=\sqrt{p},$$

или

$$|U_{a,p}|^2=U_{a,p}\overline{U}_{a,p}=\sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{x+t}{p}\right)\left(\frac{x}{p}\right)e^{2\pi i\frac{at}{p}}.$$

При $t=0$ суммирование по x даёт $p-1$; при $t>0$ оно даёт $-e^{2\pi i\frac{at}{p}}$. Поэтому

$$|U_{a,p}|^2=p-1-\sum_{t=1}^{p-1}e^{2\pi i\frac{at}{p}}=p,\ |U_{a,p}|=\sqrt{p}.$$

β) При $(a,p)=p$ теорема очевидна. При $(a,p)=1$ она следует из

$$U_{a,p}=\left(\frac{a}{p}\right)\sum_{x=1}^{p-1}\left(\frac{ax}{p}\right)e^{2\pi i\frac{ax}{p}}=\left(\frac{a}{p}\right)U_{1,p}.$$

b, α) Пусть r пробегает квадратичные вычеты, а n — квадратичные невычеты, заключённые в полной системе вычетов. Имеем

$$S_{a,p}=1+2\sum_r e^{2\pi i\frac{ar}{p}}.$$

Вычитая отсюда почленно

$$0=1+\sum_r e^{2\pi i\frac{ar}{p}}+\sum_n e^{2\pi i\frac{an}{p}},$$

мы и получим указанное равенство.

β) Имеем

$$|S_{a,m}|^2=\sum_{t=0}^{m-1}\sum_{x=0}^{m-1}e^{2\pi i\frac{a(t^2+2tx)}{m}}.$$

При данном t суммирование по x даёт $me^{2\pi i\frac{at^2}{m}}$ или 0, в зависимости от того, делится $2t$ на m или нет. При нечётном m имеем

$$|S_{a,m}|^2=me^{2\pi i\frac{a\cdot 0^2}{m}}=m.$$

При чётном $m=2m_1$ имеем

$$|S_{a,m}|^2=m\left(e^{2\pi i\frac{a\cdot 0^2}{m}}+e^{2\pi i\frac{a\cdot m_1^2}{m}}\right).$$

Здесь правая часть равна нулю при нечётном m_1 и равна $2m$ при чётном m_1.

γ) При любом целом b имеем

$$|S_{A,m}|=\left|\sum_{x=0}^{m-1}e^{2\pi i\frac{Ax^2+2Abx}{m}}\right|,$$

откуда, выбирая b из условия $2Ab\equiv a\pmod m$, мы и получим (вопрос β) указанный результат.

12, а. Имеем

$$m\sum_z{}'\,\Phi(z)=\sum_z\sum_{s=M}^{M+Q-1}\sum_{a=0}^{m-1}\Phi(z)e^{2\pi i\frac{a(z-s)}{m}}.$$

Часть суммы, стоящей справа, отвечающая $a=0$, равна $Q\sum_z \Phi(z)$; часть, отвечающая оставшимся значениям a, численно (вопрос 11, c, гл. III)

$$< \lambda \sum_{a=1}^{m-1} \left| \sum_{s=M}^{M+Q-1} e^{2\pi i \frac{-as}{m}} \right| < \lambda m (\ln m - \delta).$$

b, α) Следует из теоремы вопроса 11, a, α) и теоремы вопроса a.

β) Неравенство вопроса α) даёт $R-N=\theta\sqrt{p}\ln p$. Кроме того, очевидно, $R+N=Q$.

γ) Из теоремы вопроса 11, b, β) следует, что условия теоремы вопроса a будут соблюдены, если положим $m=p$, $\Phi(z)=1$, причём заставим z пробегать значения $z=x^2$; $x=0, 1, \ldots, p-1$. Но среди значений z имеется одно сравнимое по модулю p с 0 и по два сравнимых по модулю p с каждым квадратичным вычетом полной системы. Поэтому

$$\sum_z{}' \Phi(z)=2R, \quad \sum_z \Phi(z)=p,$$

и мы получим

$$2R=\frac{Q}{p}p+\theta\sqrt{p}\ln p.$$

b) Следует из теоремы вопроса 11, b, γ) и теоремы вопроса a.

ε) Из теоремы вопроса δ) следует, что условия теоремы вопроса a будут соблюдены, если положим $m=p$, $\Phi(z)=1$, причём заставим z пробегать значения $z=Ax^2$; $x=M_0, M_0+1, \ldots, M_0+Q_0-1$. Поэтому

$$\sum_z{}' \Phi(z)=T, \quad \sum_z \Phi(z)=Q_0,$$

откуда и следует указанная в вопросе формула.

c. Часть суммы, содержащая слагаемые с $\left(\frac{a}{p}\right)=1$, равна $p(R^2+N^2)$, оставшаяся часть равна $-2pRN$. Поэтому вся сумма равна $p(R-N)^2$.

Часть суммы, содержащая слагаемые с $a=0$, равна 0. Оставшаяся часть численно меньше (вопрос 11, c, гл. III):

$$\sum_{a=1}^{p-1} \left| \sum_{x=M}^{M+Q-1} e^{2\pi i \frac{ax}{p}} \right| \left| \sum_{a=1}^{p-1} \left| \sum_{y=M}^{M+Q-1} e^{2\pi i \frac{-ay}{p}} \right| < p^2 (\ln p)^2.$$

Следовательно, $p(R-N)^2 < p^2(\ln p)^2$, $|R-N| < \sqrt{p}\ln p$.

Решения к главе VI.

1, a. Если q — простое нечётное и $a^p \equiv 1 \pmod q$, то a по модулю q принадлежит одному из показателей $\delta=1$; p. При $\delta=1$ имеем $a \equiv 1 \pmod q$, при $\delta=p$ имеем $q-1=2px$; x — целое.

b. Если q — простое нечётное и $a^p+1 \equiv 0 \pmod q$, то $a^{2p} \equiv 1 \pmod q$. Поэтому a по модулю q принадлежит одному из показателей $\delta=1, 2, p, 2p$. Случаи $\delta=1$; p невозможны. При $\delta=2$ имеем $a^2 \equiv 1 \pmod q$, $a+1 \equiv 0 \pmod q$. При $\delta=2p$ имеем $q-1=2px$; x — целое.

c. Простыми вида $2px+1$ будут, например, простые делители числа 2^p-1. Пусть $p_1, p_2, \ldots, p_k$ — какие-либо k простых чисел вида $2px+1$; число $(p_1p_2\ldots p_k)^p-1$ имеет простой делитель вида $2px+1$, отличный от $p_1p_2\ldots p_k$.

d. Если q — простое и $2^{2^n}+1 \equiv 0 \pmod q$, то $2^{2^{n+1}} \equiv 1 \pmod q$. Поэтому 2 по модулю q принадлежит показателю 2^{n+1} и, следовательно, $q-1=2^{n+1}x$; x — целое.

2. Очевидно, a по модулю a^n-1 принадлежит показателю n. Поэтому n — делитель $\varphi(a^n-1)$.

3, a. Пусть после k-й операции снова получается исходный ряд. Очевидно, k-я операция равносильна следующей: в ряде

$$1, 2, \ldots, n-1, n, n, n-1, \ldots, 2, 1, 2, \ldots$$
$$\ldots, n-1, n, n, n-1, \ldots, 2, 1, 2, \ldots$$

берутся числа, стоящие на $1, 1+2^k, 1+2\cdot 2^k, \ldots$ местах. Поэтому на $1+2^k$ месте в исходном ряде должно стоять число 2. Следовательно, указанное в вопросе условие необходимо. Но оно и достаточно, так как при его наличии имеем следующие сравнения по модулю $2n-1$:

$$1 \equiv 1, \quad 1+2^k \equiv 0, \quad 1+2\cdot 2^k \equiv -1, \ldots$$

или же

$$1 \equiv 1, \quad 1+2^k \equiv 2, \quad 1+2\cdot 2^k \equiv 3, \ldots$$

b. Решение аналогично решению вопроса a.

4. Решение сравнения $x^\delta \equiv 1 \pmod p$ принадлежит показателю вида $\frac{\delta}{\delta'}$, где δ' — делитель δ. При этом δ' кратно d тогда и только тогда, когда $x^{\frac{\delta}{d}} \equiv 1 \pmod p$. Выписав все δ значений δ' и взяв $f=1$, получим $S'=\sum_{d\backslash\delta} \mu(d) S_d$, где S' — искомое число и $S_d=\frac{\delta}{d}$.

5, a. Здесь (§ 3; пример c, § 5) должно быть $\left(\frac{g}{2^n+1}\right)=-1$. Это требование выполняется при $g=3$.

b. Здесь не должно быть $\left(\frac{g}{2p+1}\right)=1$, $g^2 \equiv 1 \pmod{2p+1}$. Это требование выполняется при указанных значениях g.

c. Здесь не должно быть $\left(\frac{g}{4p+1}\right)=1$, $g^4 \equiv 1 \pmod{4p+1}$. Это требование выполняется при $g=2$.

d. Здесь не должно быть $\frac{g}{2^n p-1}=1$, $g^{2^n} \equiv 1 \pmod{2^n p+1}$. Это требование выполняется при $g=3$.

6, a, α) При n, кратном $p-1$, теорема очевидна. Пусть n не делится на $p-1$. Числа $1, 2, \ldots, p-1$, если отвлечься от порядка их следования, по модулю p сравнимы с числами $g, 2g, \ldots, (p-1)g$, где g — первообразный корень по модулю p. Поэтому

$$S_n \equiv g^n S_n \pmod{p}, \quad S_n \equiv 0 \pmod{p}.$$

β) Имеем

$$\sum_{x=1}^{p-1}\left(\frac{x(x^2+1)}{p}\right) \equiv \sum_{x=1}^{p-1} x^{\frac{p-1}{2}}(x^2+1)^{\frac{p-1}{2}} \pmod{p},$$

откуда (вопрос a)) и получается указанный результат.

b. При $p>2$ имеем

$$1 \cdot 2 \ldots (p-1) \equiv g^{1+2+\ldots+p-1} \equiv g^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

7, a. Имеем $g_1^{\operatorname{ind}_{g_1} a} \equiv a \pmod{p}$, $\operatorname{ind}_{g_1} a \operatorname{ind}_g g_1 \equiv \operatorname{ind}_g a \pmod{p-1}$, $\operatorname{ind}_{g_1} a \equiv \alpha \operatorname{ind}_g a \pmod{p-1}$.

b. Из $\operatorname{ind}_g a \equiv s \pmod{n}$, $\operatorname{ind}_{g_1} a \equiv \alpha \operatorname{ind}_g a \pmod{p-1}$ следует $\operatorname{ind}_{g_1} a \equiv as \equiv s_1 \pmod{n}$.

8. Пусть $(n, p-1)=1$. Найдя u из условия $nu \equiv 1 \pmod{p-1}$, получим решение $x \equiv a^u \pmod{p}$.

Пусть n — простое, $p-1=n^\alpha t$, α — целое положительное, $(t, n)=1$. Если сравнение возможно, имеем $a^{n^{\alpha-1}t} \equiv 1 \pmod{p}$; если $\alpha>1$, то, замечая, что $x \equiv g^{n^{\alpha-1}tr} \pmod{p}$, $r=0, 1, \ldots, n-1$, суть все решения сравнения $x^n \equiv 1 \pmod{p}$, при некотором $r_1=0, 1, \ldots, n-1$ имеем

$$a^{n^{\alpha-2}t} g^{n^{\alpha-1}tr_1} \equiv 1 \pmod{p};$$

если $\alpha>2$, то при некотором $r_2=0, 1, \ldots, n-1$ имеем

$$a^{n^{\alpha-3}t} g^{n^{\alpha-2}tr_1+n^{\alpha-1}tr_2} \equiv 1 \pmod{p},$$

и т. д.; наконец, при некотором $r_{\alpha-1}=0, 1, \ldots, n-1$ имеем

$$a^t g^{ntr_1+n^2tr_2+\ldots+n^{\alpha-1}tr_{\alpha-1}} \equiv 1 \pmod{p}.$$

Найдя u и v из условия $tu-nv=-1$, получим n решений:

$$x \equiv a^v g^{u(r_1+nr_2+\ldots+n^{\alpha-2}r_{\alpha-1})+n^{\alpha-1}tr} \pmod{p}; \quad r=0, 1, \ldots, n-1.$$

Пусть простое n_1 делит $(n, p-1)$, $n=n_1n_2$, $n_2>1$. Соответственно каждому решению сравнения $y^{n_1} \equiv a \pmod{p}$ разыскиваем решения сравнения $x^{n_2} \equiv y \pmod{p}$.

9, a. Указанным путём получим $cc_0c_1 \ldots c_k=\varphi(m)$ характеров. Пусть у двух характеров $\chi_1(a)$ и $\chi_2(a)$ не равны между собою значения R' и R'' какого-либо из корней $R, R_0, R_1, \ldots, R_k$; для числа a_1, у которого все индексы равны 0, кроме лишь одного, отвечающего указанным R' и R'', равного 1, имеем

$$\chi_1(a_1)=R', \quad \chi_2(a_1)=R''.$$

b, α) Имеем $\chi(1)=R^0 \ldots R_k^0=1$.

β) Пусть $\gamma', \ldots, \gamma_k'$; $\gamma'', \ldots, \gamma_k''$ — системы индексов чисел a_1 и a_2; тогда $\gamma'+\gamma'', \ldots, \gamma_k'+\gamma_k''$ — система индексов числа a_1a_2 (c, § 7).

γ) При $a_1 \equiv a_2 \pmod{m}$ индексы чисел a_1 и a_2 сравнимы между собою соответственно по модулям $c, \ldots, c_k$.

c. Указанное свойство следует из

$$\sum_{a=0}^{m-1}\chi(a)=\sum_{\gamma=0}^{c-1}R^\gamma \ldots \sum_{\gamma_k=0}^{c_k-1}R_k^{\gamma_k}.$$

d. Указанное свойство следует из

$$\sum_{\chi}\chi(a_1)=\sum_{R}R^\gamma \ldots \sum_{R_k}R_k^{\gamma_k}.$$

e. Пусть $\varphi(a_1) \gtrless 0$. Тогда $\psi(a_1)=\psi(a_1)\psi(1)$. Поэтому $\psi(1)=1$. Найдя a' из условия $aa' \equiv 1 \pmod{m}$, имеем $\psi(a)\psi(a')=1$. Поэтому $\psi(a) \gtrless 0$ при $(a, m)=1$.

При $(a_1, m)=1$ имеем

$$\sum_a{}' \frac{\chi(a)}{\psi(a)}=\sum_a{}' \frac{\chi(a_1a)}{\psi(a_1a)}=\frac{\chi(a_1)}{\psi(a_1)}\sum_a{}' \frac{\chi(a)}{\psi(a)};$$

поэтому или $\sum_a{}' \frac{\chi(a)}{\psi(a)}=0$, или же $\psi(a_1)=\chi(a_1)$ при всех a_1. Но первое предположение не может оправдываться при всех χ: тогда было бы $H=0$, а между тем $H=\varphi(m)$, так как, суммируя при данном a по всем характерам, имеем

$$\sum_\chi \frac{\chi(a)}{\psi(a)}=\begin{cases}\varphi(m), & \text{если } a \equiv 1 \pmod{m},\\ 0 & \text{в противном случае.}\end{cases}$$

f, α) Если $R', \ldots, R_k$ и $R'', \ldots, R_k''$ — значения $R, \ldots, R$ отвечающие характерам $\chi_1(a)$ и $\chi_2(a)$, то $\chi_1(a)\chi_2(a)$ — характер, у которого соответствующие значения суть $R'R'', \ldots, R_kR_k''$.

β) Когда $R, \ldots, R_k$ пробегают все корни соответствующих уравнений, то $R'R, \ldots, R_k'R_k$ пробегают в некотором порядке те же самые корни.

γ) Определяя l' из условия $ll' \equiv 1 \pmod m$, имеем

$$\sum_{\chi} \frac{\chi(x)}{\chi(l)} = \sum_{\chi} \frac{\chi(al')}{\chi(ll')} = \sum_{\chi} \chi(al'),$$

что равно $\varphi(m)$ или 0, в зависимости от того, будет ли $a \equiv l \pmod m$ или нет.

10, а. α) Определяя x' сравнением $xx' \equiv 1 \pmod p$, имеем

$$\sum_{x=1}^{p-1} e^{2\pi i \frac{l \operatorname{ind}(x-k) - l \operatorname{ind} x}{n}} = \sum_{x=1}^{p-1} e^{2\pi i \frac{l \operatorname{ind}(1+kx')}{n}} = -1.$$

β) Имеем

$$S = \sum_{x=0}^{p-1} \sum_{z_1=0}^{Q-1} \sum_{z=0}^{Q-1} e^{2\pi i \frac{l \operatorname{ind}(x+z_1) - l \operatorname{ind}(x+z)}{n}}$$

При $z_1 = z$ суммирование по x даёт $p-1$, при z_1, не равном z, суммирование по x (вопрос α)) даёт -1. Поэтому

$$S = (p-1)Q - Q(Q-1) = (p-Q)Q.$$

γ) Пусть Q_x — число чисел ряда $x+z$; $z=0, 1, \ldots, Q-1$, не делящихся на p, а $T_{n,x}$ — число чисел того же ряда, принадлежащих s-й совокупности. Пусть, наконец,

$$U_{n,x} = -\frac{Q_x}{n} + T_{n,x}, \qquad S = \sum_{x=0}^{p-1} U_{n,x}^2$$

Имеем

$$U_{n,x} = \frac{1}{n} \sum_{l=1}^{n-1} \sum_{z=0}^{Q-1} e^{2\pi i \frac{l(\operatorname{ind}(x-z) - s)}{n}} = \frac{1}{n} \sum_{l=1}^{n-1} e^{-2\pi i \frac{ls}{n}} S_{l,n,x},$$

$$U_{n,x}^2 \leqslant \frac{1}{n^2}(n-1) \sum_{l=1}^{n-1} |S_{l,n,x}|^2, \qquad S \leqslant \left(\frac{n-1}{n}\right)^2 (p-Q)Q.$$

Полагая $Q = [n\sqrt{p}]$ и допуская, что в указанном в вопросе ряде чисел s-й совокупности нет, убедимся, что $|U_{n,x}| \geqslant \frac{Q-1}{n}$ при $x = M, M+1, \ldots, M+Q-1$, и, таким образом,

$$Q\left(\frac{Q-1}{n}\right)^2 \leqslant \left(\frac{n-1}{n}\right)^2 (p-Q)Q, \quad (n\sqrt{p}-2)^2 < (n\sqrt{p}-\sqrt{p})^2,$$

что невозможно.

b. Пусть p_0 — произведение различных простых делителей числа $p-1$, Q_x — число чисел ряда $x+z$; $z=0, 1, \ldots, Q-1$, не делящихся на p, а G_x — число чисел того же ряда, являющихся первообразными корнями по модулю p. Пусть, наконец,

$$p = \left(\sum_{d \setminus p_0} \frac{\mu(d)}{d}\right)^{-1} = \frac{p-1}{\varphi(p-1)}, \quad w_x' = -\frac{Q_x}{p} + G_x, \quad \Sigma = \sum_{x=0}^{p-1} w_x^2.$$

Взяв $f(z) = 1$ и заставляя ξ пробегать значения $\xi = \operatorname{ind}(x+z)$; $z = 0, 1, \ldots, Q-1$, получим $S' = \sum_{d \setminus p_0} \mu(d) S_d$. Здесь S' — число значений ξ с условием $(\xi, p-1) = 1$; поэтому $S' = G_x$. Далее, S_d — число значений ξ, кратных d; поэтому $S_d = T_{d,x}$ (вопрос а, γ) при $s = 0$. Следовательно

$$w_x = -\frac{Q_x}{p} + \sum_{d \setminus p_0} \mu(d) T_{d,x} = \sum_{d \setminus p_0} \mu(d) U_{d,x},$$

$$w_x^2 \leqslant 2^k \sum_{d \setminus p_0} U_{d,x}^2, \qquad \Sigma < 2^{2k}(p-Q)Q.$$

Полагая $Q = [P2^k\sqrt{p}]$ и допуская, что в указанном в вопросе ряде первообразных корней нет, убедимся, что $|w_x| \geqslant \frac{Q-1}{P}$ при $x = M, M+1, \ldots, M+Q-1$ и, таким образом,

$$Q\left(\frac{Q-1}{P}\right)^2 \leqslant 2^{2k}(p-Q)Q, \quad (P2^k\sqrt{p}-2)^2 < \left(P2^k\sqrt{p} - \frac{P2^kQ}{2\sqrt{p}}\right)^2,$$

что невозможно.

11, а, α). Имеем

$$|U_{a,p}|^2 = \sum_{t=1}^{p-1} \sum_{x=1}^{p-1} e^{2\pi i \frac{k \operatorname{ind} t}{n}} e^{2\pi i \frac{a(t-1)x}{p}} =$$

$$= p - 1 - \sum_{t=2}^{p-1} e^{2\pi i \frac{k \operatorname{ind} t}{n}} = p.$$

β) При $(a, p)=p$ теорема очевидна. При $(a, p)=1$ она следует из

$$U_{a,p}=e^{2\pi i\frac{-k\operatorname{ind} a}{n}}\sum_{x=1}^{p-1}e^{2\pi i\frac{k\operatorname{ind} ax}{n}}e^{2\pi i\frac{ax}{p}}=e^{2\pi i\frac{-k\operatorname{ind} a}{n}}U_{1,p}.$$

γ) Очевидно, A и B — целые, причём $|S|^2=A^2+B^2$. При некоторых ε, ε', ε'' с условием $|\varepsilon|=|\varepsilon'|=|\varepsilon''|=1$ имеем (вопрос β))

$$S=\frac{1}{\varepsilon\sqrt{p}\,\varepsilon'\sqrt{p}}\sum_{z_1=1}^{p-1}\sum_{z=1}^{p-1}\sum_{x=0}^{p-1}e^{-2\pi i\frac{\operatorname{ind} z_1+\operatorname{ind} z}{4}}e^{2\pi i\frac{z_1x+z(x+1)}{p}}.$$

Если z_1+z не равно p, суммирование по x даёт нуль. Поэтому

$$S=\varepsilon''\sum_{z=1}^{p-1}\left(\frac{z}{p}\right)e^{2\pi i\frac{z}{p}}=\varepsilon''\sqrt{p},\quad |S|^2=p.$$

b, α) При данном z сравнение $x^n\equiv z\pmod p$ возможно лишь в случае, когда $\operatorname{ind} z$ делится на δ, причём тогда это сравнение имеет δ решений. Поэтому при $\delta=1$ имеем $S_{a,p}=0$. Если же $\delta>1$, то имеем

$$S_{a,p}=1+\sum_{k=0}^{\delta-1}\sum_{z=1}^{p-1}e^{2\pi i\frac{k\operatorname{ind} z}{\delta}}e^{2\pi i\frac{az}{p}}$$

При $k=0$ суммирование по z даёт -1; при $k>0$ оно даёт величину, модуль которой равен $\sqrt{p}$. Отсюда и следует результат, указанный в вопросе.

β) Полагая

$$x=u+p^{s-1}v;\quad u=0,\ \ldots,\ p^{s-1}-1,\quad v=0,\ \ldots,\ p-1,$$

имеем

$$e^{2\pi i\frac{ax^n}{p^s}}=e^{2\pi ia\,(u^np^{-s}+nu^{n-1}p^{-1}v)}.$$

При $(u,\ p)=1$ суммирование по v даёт нуль. Поэтому

$$S_{a,\,p^s}=\sum_{x_0=0}^{p^{s-1}-1}e^{2\pi i\frac{ax_0^n}{p^s}}=p^{n-1}S_{a,\,p^{s-n}},\ S'_{a,\,p^s}=0.$$

γ) Пусть p^τ — наибольшая степень p, делящая n. Имеем $s\geqslant\tau+3$. Полагая

$$x=u+p^{s-1-\tau}v;\ u=0,\ \ldots,\ p^{s-1-\tau}-1,\ v=0,\ \ldots,\ p^{\tau+1}-1,$$

находим

$$e^{2\pi i\frac{ax^n}{p^s}}=e^{2\pi ia\,(u^np^{-s}+nu^{n-1}p^{-\tau-1}v)}.$$

При $(u,\ p)=1$ суммирование по v даёт нуль. Поэтому

$$S_{a,\,p^s}=\sum_{x_0=0}^{p^{s-1}-1}e^{2\pi i\frac{ax_0^n}{p^{s-n}}}=p^{n-1}S_{a,\,p^{s-n}},S'_{a,\,p^s}=0.$$

δ) Пусть $m=p_1^{\alpha_1}\ldots p_k^{\alpha_k}$ — каноническое разложение числа m. Полагая

$$T_{a,\,m}=m^{-1+\nu}S_{a,\,m};\quad \nu=\frac{1}{n},\ m=M_1p_1^{\alpha_1}=\ldots=M_kp_k^{\alpha_k}$$

и определяя $a_1,\ \ldots,\ a_k$ из условия $a\equiv M_1a_1+\ldots+M_ka_k\pmod m$, имеем (вопрос 12, d, гл. III)

$$T_{a,\,m}=T_{a_1,\,p_1^{\alpha_1}}\ldots T_{a_k,\,p^{\alpha_k}}.$$

Но при $s=1$ имеем

$$|T_{a,\,p^s}|<p^{-1+\nu}n\sqrt{p}\leqslant np^{-\frac{1}{6}}.$$

При $1<s\leqslant n$, $(n,\ p)=1$ имеем

$$|T_{a,\,p^s}|=p^{-s+s\nu}p^{s-1}\leqslant 1.$$

При $1<s\leqslant n$, $(n,\ p)=p$ имеем

$$|T_{a,\,p^s}|\leqslant p^{-s+s\nu}p^s\leqslant p<n.$$

Случай $s>n$ ввиду $T_{a,\,p^s}=p^{-s+s\nu}p^{n-1}S_{a,\,p^{s-n}}=T_{a,\,p^{s-n}}$ сводится к случаю $s\leqslant n$. Поэтому

$$|T_{a,\,m}|\leqslant C=n^{6}+n,$$

откуда и получается указанное в вопросе неравенство.

12, a. Следует из теоремы вопроса 11, a, α) и теоремы вопроса 12, a, гл. V.

b. Имеем

$$Tn=\sum_{x=M}^{M+Q-1}\sum_{k=0}^{n-1} e^{2\pi i\frac{k(\operatorname{ind}x-s)}{n}}.$$

При $k=0$, суммируя по x, получим Q; при $k>0$ получим число, модуль которого $<\sqrt{p}\ln p$. Отсюда и следует указанная в вопросе формула.

c. Взяв $f(x)=1$ и заставляя x пробегать значения $x=\operatorname{ind}M$, $\operatorname{ind}(M+1)$, ..., $\operatorname{ind}(M+Q-1)$, получим (вопрос 17, a, гл. II)

$S'=\sum_{d\setminus p-1}\mu(d)S_d$. Здесь S' — число значений x с условием $(x,\ p-1)=1$; поэтому $S'=T$. Далее S_d — число значений x, кратных d, т. е. число вычетов степени d в ряде M, $M+1$, ..., $M+Q-1$. Следовательно,

$$H=\sum_{d\setminus p-1}\mu(d)\left(\frac{Q}{d}+\vartheta_d\sqrt{p}\ln p\right);\ |\vartheta_d|<1,\ \vartheta_1=0.$$

d. Из теоремы вопроса a следует, что условия вопроса 12, a, гл. V будут соблюдены, если положим $m=p-1$, $\Phi(z)=1$, причём заставим z пробегать значения $z=\operatorname{ind}x$; $x=M$, $M+1$, ..., $M+Q-1$. Тогда получим (Q_1 вместо Q)

$$\sum_z{}'\Phi(z)=J,\quad \sum_z\Phi(z)=Q,\quad J=\frac{Q_1}{p-1}Q+\vartheta\sqrt{p}(\ln p)^2.$$

13. Допустим, что невычетов, не превосходящих h, нет. Число невычетов степени n среди чисел

$$1,\ \ldots,\ Q;\ Q=\sqrt{p}(\ln p)^2$$

можно оценить двумя способами: исходя из формулы вопроса 12, b и исходя из того, что невычетами могут быть лишь числа, делящиеся на простые, большие h. Получим

$$1-\frac{1}{n}<\ln\frac{\frac{1}{2}\ln p+2\ln\ln p}{\frac{1}{c}\ln p+2\ln\ln p}+O\left(\frac{1}{\ln p}\right),$$

$$0<\ln\frac{1+4\frac{\ln\ln p}{\ln p}}{1+2c\frac{\ln\ln p}{\ln p}}+O\left(\frac{1}{\ln p}\right).$$

Невозможность последнего неравенства при всех достаточно больших p и доказывает теорему.

14, a. Имеем

$$|S|^2\leqslant X\sum_{x=0}^{m-1}\sum_{y_1=0}^{m-1}\sum_{y=0}^{m-1}\rho(y_1)\overline{\rho(y)}\,e^{2\pi i\frac{ax(y_1-y)}{m}}.$$

При данных y_1 и y суммирование по x даёт $Xm\,|\rho(y)|^2$ или нуль, в зависимости от того, будет ли $y_1=y$ или нет. Поэтому

$$|S|^2\leqslant XYm,\quad |S|\leqslant\sqrt{XYm}.$$

b, a) Имеем

$$S=\frac{1}{\varphi(m)}\sum_u\sum_v\chi(u)\chi(v)\,e^{2\pi i\frac{au^nv^n}{m}},$$

где u и v пробегают приведённые системы вычетов по модулю m. Отсюда

$$S=\frac{1}{\varphi(m)}\sum_{x=0}^{m-1}\sum_{y=0}^{m-1}\nu(x)\rho(y)\,e^{2\pi i\frac{axy}{m}};$$

$$\nu(x)=\sum_{u^n\equiv x\,(\mathrm{mod}\,m)}\chi(u),\qquad \rho(y)=\sum_{v^n\equiv y\,(\mathrm{mod}\,m)}\chi(v).$$

Но имеем (вопрос 11, гл. IV)

$$\sum_{x=0}^{m-1}|\nu(x)|^2\leqslant K\varphi(m),\qquad \sum_{y=0}^{m-1}|\rho(y)|^2\leqslant K\varphi(m).$$

Поэтому (вопрос a)

$$|S|\leqslant\frac{1}{\varphi(m)}\sqrt{K\varphi(m)K\varphi(m)m}=K\sqrt{m}.$$

β) Пусть $m=2^\alpha p_1^{\alpha_1}\ldots p_k^{\alpha_k}$ — каноническое разложение числа m. Сравнение $x^n\equiv1\,(\mathrm{mod}\,m)$ равносильно системе

$$x^n\equiv1\,(\mathrm{mod}\,2^\alpha),\ x^n\equiv1\,(\mathrm{mod}\,p_1^{\alpha_1}),\ \ldots,\ x^n\equiv1\,(\mathrm{mod}\,p_k^{\alpha_k}).$$

Пусть $\gamma(x)$ и $\gamma_0(x)$ — индексы числа x по модулю 2^α (g, § 6). Сравнение $x^n\equiv1\,(\mathrm{mod}\,2^\alpha)$ равносильно системе $n\gamma(x)\equiv0\,(\mathrm{mod}\,c)$, $n\gamma_0(x)\equiv0\,(\mathrm{mod}\,c_0)$. Первое сравнение этой системы имеет не более 2 решений; второе — не более n решений. Поэтому сравнение $x^n\equiv1\,(\mathrm{mod}\,2^\alpha)$ имеет не более $2n$ решений. Согласно b, § 5

каждое из сравнений $x^n \equiv 1 \pmod{p_1^{\alpha_1}}, \ldots, x^n \equiv 1 \pmod{p_k^{\alpha_k}}$ имеет не более n решений. Следовательно,

$$K \leqslant 2\,(\tau(m))^{\frac{\ln n}{\ln 2}};\ K = O(m^\varepsilon).$$

15, a. Имеем

$$|S|^2 = \sum_{t=1}^{p-1}\sum_{x=1}^{p-1} e^{2\pi i \frac{a(t^n-1)x^n + b(t-1)x}{p}}.$$

Если $t^n \equiv 1 \pmod p$, то суммирование по x даёт $p-1$ при $t \equiv 1 \pmod p$ и -1 в остальных случаях. В противном случае, беря $z(t-1)^{-1}$ вместо x, соответствующую выбранному t часть двойной суммы представим в форме

$$\sum_{z=1}^{p-1} e^{2\pi i \frac{bz}{p}} e^{2\pi i \frac{a(t^n-1)(t-1)^{-n} z^n}{p}}$$

Поэтому

$$|S|^2 \leqslant p-1 + \left| \sum_{u=1}^{p-1}\sum_{v=1}^{p-1} \nu(u)\,\rho(v)\, e^{2\pi i \frac{auv}{p}} \right|,$$

где $\nu(u)$ равно числу решений сравнения $(t^n-1)(t-1)^{-n} \equiv u \pmod p$, а $|\rho(v)|$ не превосходит числа решений сравнения $z^n \equiv v \pmod p$. Поэтому $\nu(u) \leqslant 2n_1$, $|\rho(v)| \leqslant n_1$,

$$\sum_{u=1}^{p-1} |\nu(u)|^2 \leqslant (p-1)\,2n_1, \qquad \sum_{v=1}^{p-1} |\rho(v)|^2 \leqslant (p-1)\,n_1.$$

Применяя теорему вопроса 14, a, получим

$$|S|^2 \leqslant p-1+\sqrt{(p-1)\,2n_1\,(p-1)\,n_1 p} < 2n_1 p^{\frac{3}{2}}.$$

b, α) Следует из теоремы вопроса a и теоремы вопроса **12, a, гл. V.**

β) Из теоремы вопроса α) следует, что условия теоремы вопроса **12, a, гл. V** будут соблюдены, если положим $m = p$, $\Phi(z) = 1$, причём заставим z пробегать значения $z = Ax^n$; $x = M_0$, $M_0+1, \ldots, M_0+Q_0-1$. Поэтому

$$\sum_z{}' \Phi(z) = T, \quad \sum_z \Phi(z) = Q_0,$$

откуда и следует указанная в вопросе формула.

c, α) Пусть $\gamma \equiv 4a\gamma_1 \pmod p$. Имеем (вопрос 11, a, гл. V)

$$\left(\frac{a}{p}\right) S = \sum_{x=0}^{p-1} \left(\frac{4a^2x^2+4abx+4ac}{p}\right) e^{2\pi i \frac{4a\gamma_1 x}{p}} =$$

$$= \frac{1}{U_{1,p}} \sum_{z=1}^{p-1} \left(\frac{z}{p}\right) \sum_{x=0}^{p-1} e^{2\pi i \frac{z(4a^2x^2+4abx+4ac+4a\gamma_1 xz^{-1})}{p}} =$$

$$= \sum_{z=1}^{p-1} e^{2\pi i \frac{-(b^2-4ac)z - 2b\gamma_1 - \gamma_1^2 z^{-1}}{p}}.$$

Последняя же сумма (вопрос a) численно $< \frac{3}{2} p^{\frac{3}{4}}$.

β) Следует из теоремы вопроса α) и теоремы вопроса **12, a, гл. V.**

ОТВЕТЫ К ЧИСЛЕННЫМ ПРИМЕРАМ.

Ответы к главе I.

1, a. 17.
b. 23.

2, a. α) $\delta_4 = \frac{15}{11}$; β) $\alpha = \frac{19}{14} + \frac{9}{14 \cdot 20}$.

b, α) $\delta_6 = \frac{80}{59}$; β) $\alpha = \frac{1002}{739} + \frac{9}{739 \cdot 1000}$.

3. Всего получим 22 дроби.
5, a. $2^3 \cdot 3^5 \cdot 11^3$.
b. $2^3 \cdot 3^3 \cdot 5^4 \cdot 7^3 \cdot 11^3 \cdot 17 \cdot 23 \cdot 37$.

Ответы к главе II.

1, a. 13 142.
b. $2^{119} \cdot 3^{59} \cdot 5^{31} \cdot 7^{19} \cdot 11^{12} \cdot 13^9 \cdot 17^7 \cdot 19^5 \cdot 23^5 \cdot 29^4 \cdot 31^4 \cdot 37^3 \times \times 41^3 \cdot 43^3 \cdot 47^2 \cdot 53^2 \cdot 59^2 \cdot 61^2 \cdot 67 \cdot 71 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97 \times \times 101 \cdot 103 \cdot 107 \cdot 109 \cdot 113$.
2, a. $\tau(5600) = 36$; $S(5600) = 15\,624$
b. $\tau(116\,424) = 96$; $S(116\,424) = 410\,400$
3. Сумма всех значений равна 1.
4. α) 1152; β) 466 400.
5. Сумма всех значений равна 774.

Ответы к главе III.

1, a. 70.
b. Делится.
2, a. $3^3 \cdot 5^3 \cdot 11^3 \cdot 2999$.
b. $7 \cdot 13 \cdot 37 \cdot 73 \cdot 101 \cdot 137 \cdot 17 \cdot 19 \cdot 257$

Ответы к главе IV.

1, a. $x \equiv 81 \pmod{337}$.
b. $x \equiv 200$; 751; 1302; 1853; 2404 (mod 2755).
2, b. $x \equiv 1630 \pmod{2413}$.
3. $x = 94 + 111t$; $y = 39 + 47t$, где t — любое целое.

4, a. $x \equiv 170b_1 + 52b_2 \pmod{221}$; $x \equiv 131 \pmod{221}$;
$x \equiv 110 \pmod{221}$; $x \equiv 89 \pmod{221}$.
b. $x \equiv 11\,151b_1 + 11\,800b_2 + 16\,875b_3 \pmod{39\,825}$.
5, a. $x \equiv 91 \pmod{120}$.
b. $x \equiv 8479 \pmod{15\,015}$.
6. $x \equiv 100 \pmod{143}$; $y \equiv 111 \pmod{143}$.
7, a $3x^4 + 2x^3 + 3x^2 + 2x \equiv 0 \pmod 5$.
b. $x^5 + 5x^4 + 3x^3 + 3x + 2 \equiv 0 \pmod 7$.
8. $x^8 + 4x^5 + 22x^4 + 76x^3 + 70x^2 + 52x + 39 \equiv 0 \pmod{101}$.
9, a. $x \equiv 16 \pmod{27}$.
b. $x \equiv 22$; 53 (mod 64).
10, a. $x \equiv 113 \pmod{125}$.
b. $x \equiv 43$, 123, 168, 248, 293, 373, 418, 498, 543, 623 (mod 625).
11. a. $x \equiv 2$, 5, 11, 17, 20, 26 (mod 30).
b. $x \equiv 76$, 22, 176, 122 (mod 225).

Ответы к главе V.

1, a. 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18.
b. 2, 5, 6, 8, 13, 14, 15, 17, 18, 19, 20, 22, 23, 24, 29, 31, 32, 35.
2, a. α) 0; β) 2.
b. α) 0; β) 2.
3, a. α) 0; β) 2.
b. α) 0; β) 2.
4, a. α) $x \equiv \pm 9 \pmod{19}$; β) $x \equiv \pm 11 \pmod{29}$;
γ) $x \equiv \pm 14 \pmod{97}$.
b. α) $x \equiv \pm 66 \pmod{311}$; β) $x \equiv \pm 130 \pmod{277}$;
γ) $x \equiv \pm 94 \pmod{353}$.
5, a. $x \equiv \pm 72 \pmod{125}$.
b. $x \equiv \pm 127 \pmod{243}$.
6, a. $x \equiv 13$, 19, 45, 51 (mod 64).
b. $x \equiv 41$, 87, 169, 215 (mod 256).

Ответы к главе VI.

1, a. 6.
b. 18.
2, a. 3, 3, 3.
b. 5, 5, 5.
c. 7.
5, a. α) 0; β) 1; γ) 3.
b. α) 0; β) 1; γ) 10.
6, a. α) $x \equiv 40$; 27 (mod 67), β) $x \equiv 33 \pmod{67}$,
γ) $x \equiv 8$, 36, 28, 59, 31, 39 (mod 67).
b. α) $x \equiv 17 \pmod{73}$, β) $x \equiv 50$, 12, 35, 23, 61, 38 (mod 73),
γ) $x \equiv 3$, 24, 46 (mod 73).

7, a. α) 0; β) 4.
b. α) 0; β) 7.
8, a. α) $x \equiv 54 \pmod{101}$. β) $x \equiv 53, 88, 90, 66, 8 \pmod{101}$.
b. $x \equiv 59, 11, 39 \pmod{109}$.
9, a. α) 1, 4, 5, 6, 7, 9, 11, 16, 17; β) 1, 7, 8, 11, 12, 18.
b. α) 1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36;
β) 1, 7, 9, 10, 12, 16, 26, 33, 34.
10, a. α) 7, 37; β) 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34.
b. α) 3, 27, 41, 52;
β) 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59.

ТАБЛИЦЫ ИНДЕКСОВ.

Простое число 3.

N	0	1	2	3	4	5	6	7	8	9
0		0	1							

I	0	1	2	3	4	5	6	7	8	9
0	1	2								

Простое число 5.

N	0	1	2	3	4	5	6	7	8	9
0		0	1	3	2					

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	3						

Простое число 7.

N	0	1	2	3	4	5	6	7	8	9
0		0	2	1	4	5	3			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	2	6	4	5				

Простое число 11.

N	0	1	2	3	4	5	6	7	8	9
0		0	1	8	2	4	9	7	3	6
1	5									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	5	10	9	7	3	6
1										

Простое число 13.

N	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8
1	10	7	6							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	3	6	12	11	9	5
1	10	7								

Простое число 17.

N	0	1	2	3	4	5	6	7	8	9
0		0	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	10	13	5	15	11	16	14
1	8	7	4	12	2	6				

Простое число 19.

N	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	13	7	14	9	18
1	17	15	11	3	6	12	5	10		

Простое число 23.

N	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	19	3	15	6	7
2	12	14								

Простое число 29.

N	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15		

Простое число 31.

N	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2
1	14	23	19	11	22	21	6	7	26	4
2	8	29	17	27	13	10	5	3	16	9
3	15									

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	19	26	16	17	20	29
1	25	13	8	24	10	30	28	22	4	12
2	5	15	14	11	2	6	18	23	7	21

Простое число 37.

N	0	1	2	3	4	5	6	7	8	9
0		0	1	26	2	23	27	32	3	16
1	24	30	28	11	33	13	4	7	17	35
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	27	17	34	31
1	25	13	26	15	30	23	9	18	36	35
2	33	29	21	5	10	20	3	6	12	24
3	11	22	7	14	28	19				

Простое число 41.

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

Простое число 43.

N	0	1	2	3	4	5	6	7	8	9
0		0	27	1	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	38	28	41	37	25	32
1	10	30	4	12	36	22	23	26	35	19
2	14	42	40	34	16	5	15	2	6	18
3	11	33	13	39	31	7	21	20	17	8
4	24	29								

Простое число 47.

N	0	1	2	3	4	5	6	7	8	9
0		0	18	20	36	1	38	32	8	40
1	19	7	10	11	4	21	26	16	12	45
2	37	6	25	5	28	2	29	14	22	35
3	39	3	44	27	34	33	30	42	17	31
4	9	15	24	13	43	41	23			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	31	14	23	21	11	8	40
1	12	13	18	43	27	41	17	38	2	10
2	3	15	28	46	42	22	16	33	24	26
3	36	39	7	35	34	29	4	20	6	30
4	9	45	37	44	32	19				

Простое число 53.

N	0	1	2	3	4	5	6	7	8	9
0		0	1	17	2	47	18	14	3	34
1	48	6	19	24	15	12	4	10	35	37
2	49	31	7	39	20	42	25	51	16	46
3	13	33	5	23	11	9	36	30	38	41
4	50	45	32	22	8	29	40	44	21	28
5	43	27	26							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	11	22	44	35
1	17	34	15	30	7	14	28	3	6	12
2	24	48	43	33	13	26	52	51	49	45
3	37	21	42	31	9	18	36	19	38	23
4	46	39	25	50	47	41	29	5	10	20
5	40	27								

Простое число 59.

N	0	1	2	3	4	5	6	7	8	9
0		0	1	50	2	6	51	18	3	42
1	7	25	52	45	19	56	4	40	43	38
2	8	10	26	15	53	12	46	34	20	28
3	57	49	5	17	41	24	44	55	39	37
4	9	14	11	33	27	48	16	23	54	36
5	13	32	47	22	35	31	21	30	29	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	5	10	20	40
1	21	42	25	50	41	23	46	33	7	14
2	28	56	53	47	35	11	22	44	29	58
3	57	55	51	43	27	54	49	39	19	38
4	17	34	9	18	36	13	26	52	45	31
5	3	6	12	24	48	37	15	30		

Простое число 61.

N	0	1	2	3	4	5	6	7	8	9
0		0	1	6	2	22	7	49	3	12
1	23	15	8	40	50	28	4	47	13	26
2	24	55	16	57	9	44	41	18	51	35
3	29	59	5	21	48	11	14	39	27	46
4	25	54	56	43	17	34	58	20	10	38
5	45	53	42	33	19	37	52	32	36	31
6	30									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	3	6	12	24
1	48	35	9	18	36	11	22	44	27	54
2	47	33	5	10	20	40	19	38	15	30
3	60	59	57	53	45	29	58	55	49	37
4	13	26	52	43	25	50	39	17	34	7
5	14	28	56	51	41	21	42	23	46	31

Простое число 67.

N	0	1	2	3	4	5	6	7	8	9
0		0	1	39	2	15	40	23	3	12
1	16	59	41	19	24	54	4	64	13	10
2	17	62	60	28	42	30	20	51	25	44
3	55	47	5	32	65	38	14	22	11	58
4	18	53	63	9	61	27	29	50	43	46
5	31	37	21	57	52	8	26	49	45	36
6	56	7	48	35	6	34	33			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	61	55	43
1	19	38	9	18	36	5	10	20	40	13
2	26	52	37	7	14	28	56	45	23	46
3	25	50	33	66	65	63	59	51	35	3
4	6	12	24	48	29	58	49	31	62	57
5	47	27	54	41	15	30	60	53	39	11
6	22	44	21	42	17	34				

Простое число 71.

N	0	1	2	3	4	5	6	7	8	9
0		0	6	26	12	28	32	1	18	52
1	34	31	38	39	7	54	24	49	58	16
2	40	27	37	15	44	56	45	8	13	68
3	60	11	30	57	55	29	64	20	22	65
4	46	25	33	48	43	10	21	9	50	2
5	62	5	51	23	14	59	19	42	4	3
6	66	69	17	53	36	67	63	47	61	41
7	35									

I	0	1	2	3	4	5	6	7	8	9
0	1	7	49	59	58	51	2	14	27	47
1	45	31	4	28	54	23	19	62	8	56
2	37	46	38	53	16	41	3	21	5	35
3	32	11	6	42	10	70	64	22	12	13
4	20	69	57	44	24	26	40	67	43	17
5	48	52	9	63	15	34	25	33	18	55
6	30	68	50	66	36	39	60	65	29	61

Простое число 73.

N	0	1	2	3	4	5	6	7	8	9
0		0	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44								

Простое число 79.

N	0	1	2	3	4	5	6	7	8	9
0		0	4	1	8	62	5	53	12	2
1	66	68	9	34	57	63	16	21	6	32
2	70	54	72	26	13	46	38	3	61	11
3	67	56	20	69	25	37	10	19	36	35
4	74	75	58	49	76	64	30	59	17	28
5	50	22	42	77	7	52	65	33	15	31
6	71	45	60	55	24	18	73	48	29	27
7	41	51	14	44	23	47	40	43	39	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	2	6	18	54	4	12
1	36	29	8	24	72	58	16	48	65	37
2	32	17	51	74	64	34	23	69	49	68
3	46	59	19	57	13	39	38	35	26	78
4	76	70	52	77	73	61	25	75	67	43
5	50	71	55	7	21	63	31	14	42	47
6	62	28	5	15	45	56	10	30	11	33
7	20	60	22	66	40	41	44	53		

Простое число 83.

N	0	1	2	3	4	5	6	7	8	9
0		0	1	72	2	27	73	8	3	62
1	28	24	74	77	9	17	4	56	63	47
2	29	60	25	60	75	54	78	52	10	12
3	18	38	5	14	57	35	64	20	48	67
4	30	40	81	71	26	7	61	23	76	16
5	55	46	79	59	53	51	11	37	13	34
6	19	66	39	70	6	22	15	45	58	50
7	36	33	65	69	21	44	49	32	68	43
8	31	42	41							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	45	7	14
1	28	56	29	58	33	66	49	15	30	60
2	37	74	65	47	11	22	44	5	10	20
3	40	80	77	71	59	35	70	57	31	62
4	41	82	81	79	75	67	51	19	38	76
5	69	55	27	54	25	50	17	34	68	53
6	23	46	9	18	36	72	61	39	78	73
7	63	43	3	6	12	24	48	13	26	52
8	21	42								

Простое число 89.

N	0	1	2	3	4	5	6	7	8	9
0		0	16	1	32	70	17	81	48	2
1	86	84	33	23	9	71	64	6	18	35
2	14	82	12	57	49	52	39	3	25	59
3	87	31	80	85	22	63	34	11	51	24
4	30	21	10	29	28	72	73	54	65	74
5	68	7	55	78	19	66	41	36	75	43
6	15	69	47	83	8	5	13	56	38	58
7	79	62	50	20	27	53	67	77	40	42
8	46	4	37	61	26	76	45	60	44	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	81	65	17	51	64	14
1	42	37	22	66	20	60	2	6	18	54
2	73	41	34	13	39	28	84	74	44	43
3	40	31	4	12	36	19	57	82	68	26
4	78	56	79	59	88	86	80	62	8	24
5	72	38	25	75	47	52	67	23	69	29
6	87	83	71	35	16	48	55	76	50	61
7	5	15	45	46	49	58	85	77	53	70
8	32	7	21	63	11	33	10	30		

Простое число 97.

N	0	1	2	3	4	5	6	7	8	9
0		0	34	70	68	1	8	31	6	44
1	35	86	42	25	65	71	40	89	78	81
2	69	5	24	77	76	2	59	18	3	13
3	9	46	74	60	27	32	16	91	19	95
4	7	85	39	4	58	45	15	84	14	62
5	36	83	93	10	52	87	37	55	47	67
6	43	64	80	75	12	26	94	57	61	51
7	66	11	50	28	29	72	53	21	33	30
8	41	88	23	17	73	90	38	83	92	54
9	79	56	49	20	22	82	48			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	28	43	21	8	40	6	30
1	53	71	64	29	48	46	36	83	27	38
2	93	77	94	82	22	13	65	34	73	74
3	79	7	35	78	2	10	50	56	86	42
4	16	80	12	60	9	45	31	58	96	92
5	72	69	54	76	89	57	91	67	44	26
6	33	68	49	51	61	14	70	59	4	20
7	3	15	75	84	32	63	24	23	18	90
8	62	19	95	87	47	41	11	55	81	17
9	85	37	88	52	66	39				

Таблица простых чисел <4000 и их наименьших первообразных корней.

p	g	p	g	p	g	p	g	p	g	p	g	p	g
2	1	179	2	419	2	661	2	947	2	1 229	2	1 523	2
3	2	181	2	421	2	673	5	953	3	1 231	3	1 531	2
5	2	191	19	431	7	677	2	967	5	1 237	2	1 543	5
7	3	193	5	433	5	683	5	971	6	1 249	7	1 549	2
11	2	197	2	439	15	691	3	977	3	1 259	2	1 553	3
13	2	199	3	443	2	701	2	983	5	1 277	2	1 559	19
17	3	211	2	449	3	709	2	991	6	1 279	3	1 567	3
19	2	223	3	457	13	719	11	997	7	1 283	2	1 571	2
23	5	227	2	461	2	727	5	1 009	11	1 289	6	1 579	3
29	2	229	6	463	3	733	6	1 013	3	1 291	2	1 583	5
31	3	233	3	467	2	739	3	1 019	2	1 297	10	1 597	11
37	2	239	7	479	13	743	5	1 021	10	1 301	2	1 601	3
41	6	241	7	487	3	751	3	1 031	14	1 303	6	1 607	5
43	3	251	6	491	2	757	2	1 033	5	1 307	2	1 609	7
47	5	257	3	499	7	761	6	1 039	3	1 319	13	1 613	3
53	2	263	5	503	5	769	11	1 049	3	1 321	13	1 619	2
59	2	269	2	509	2	773	2	1 051	7	1 327	3	1 621	2
61	2	271	6	521	3	787	2	1 061	2	1 361	3	1 627	3
67	2	277	5	523	2	797	2	1 063	3	1 367	5	1 637	2
71	7	281	3	541	2	809	3	1 069	6	1 373	2	1 657	11
73	5	283	3	547	2	811	3	1 087	3	1 381	2	1 663	3
79	3	293	2	557	2	821	2	1 091	2	1 399	13	1 667	2
83	2	307	5	563	2	823	3	1 093	5	1 409	3	1 669	2
89	3	311	17	569	3	827	2	1 097	3	1 423	3	1 693	2
97	5	313	10	571	3	829	2	1 103	5	1 427	2	1 697	3
101	2	317	2	577	5	839	11	1 109	2	1 429	6	1 699	3
103	5	331	3	587	2	853	2	1 117	2	1 433	3	1 709	3
107	2	337	10	593	3	857	3	1 123	2	1 439	7	1 721	3
109	6	347	2	599	7	859	2	1 129	11	1 447	3	1 723	3
113	3	349	2	601	7	863	5	1 151	17	1 451	2	1 733	2
127	3	353	3	607	3	877	2	1 153	5	1 453	2	1 741	2
131	2	359	7	613	2	881	3	1 163	5	1 459	5	1 747	2
137	3	367	6	617	3	883	2	1 171	2	1 471	6	1 753	7
139	2	373	2	619	2	887	5	1 181	7	1 481	3	1 759	6
149	2	379	2	631	3	907	2	1 187	2	1 483	2	1 777	5
151	6	383	5	641	3	911	17	1 193	3	1 487	5	1 783	10
157	5	389	2	643	11	919	7	1 201	11	1 489	14	1 787	2
163	2	397	5	647	5	929	3	1 213	2	1 493	2	1 789	6
167	5	401	3	653	2	937	5	1 217	3	1 499	2	1 801	11
173	2	409	21	659	2	941	2	1 223	5	1 511	11	1 811	6

Продолжение

p	g	p	g	p	g	p	g	p	g	p	g	p	g
1 823	5	2 129	3	2 417	3	2 729	3	3 049	11	3 373	5	3 691	2
1 831	3	2 131	2	2 423	5	2 731	3	3 061	6	3 389	3	3 697	5
1 847	5	2 137	10	2 437	2	2 741	2	3 067	2	3 391	3	3 701	2
1 861	2	2 141	2	2 441	6	2 749	6	3 079	6	3 407	5	3 709	2
1 867	2	2 143	3	2 447	5	2 753	3	3 083	2	3 413	2	3 719	7
1 871	14	2 153	3	2 459	2	2 767	3	3 089	3	3 433	5	3 727	3
1 873	10	2 161	23	2 467	2	2 777	3	3 109	6	3 449	3	3 733	2
1 877	2	2 179	7	2 473	5	2 789	2	3 119	7	3 457	7	3 739	7
1 879	6	2 203	5	2 477	2	2 791	6	3 121	7	3 461	2	3 761	3
1 889	3	2 207	5	2 503	3	2 797	2	3 137	3	3 463	3	3 767	5
1 901	2	2 213	2	2 521	17	2 801	3	3 163	3	3 467	2	3 769	7
1 907	2	2 221	2	2 531	2	2 803	2	3 167	5	3 469	2	3 779	2
1 913	3	2 237	2	2 539	2	2 819	2	3 169	7	3 491	2	3 793	5
1 931	2	2 239	3	2 543	5	2 833	5	3 181	7	3 499	2	3 797	2
1 933	5	2 243	2	2 549	2	2 837	2	3 187	2	3 511	7	3 803	2
1 949	2	2 251	7	2 551	6	2 843	2	3 191	11	3 517	2	3 821	3
1 951	3	2 267	2	2 557	2	2 851	2	3 203	2	3 527	5	3 823	3
1 973	2	2 269	2	2 579	2	2 857	11	3 209	3	3 529	17	3 833	3
1 979	2	2 273	3	2 591	7	2 861	2	3 217	5	3 533	2	3 847	5
1 987	2	2 281	7	2 593	7	2 879	7	3 221	10	3 539	2	3 851	2
1 993	5	2 287	19	2 609	3	2 887	5	3 229	6	3 541	7	3 853	2
1 997	2	2 293	2	2 617	5	2 897	3	3 251	6	3 547	2	3 863	5
1 999	3	2 297	5	2 621	2	2 903	5	3 253	2	3 557	2	3 877	2
2 003	5	2 309	2	2 633	3	2 909	2	3 257	3	3 559	3	3 881	13
2 011	3	2 311	3	2 647	3	2 917	5	3 259	3	3 571	2	3 889	11
2 017	5	2 333	2	2 657	3	2 927	5	3 271	3	3 581	2	3 907	2
2 027	2	2 339	2	2 659	2	2 939	2	3 299	2	3 583	3	3 911	13
2 029	2	2 341	7	2 663	5	2 953	13	3 301	6	3 593	3	3 917	2
2 039	7	2 347	3	2 671	7	2 957	2	3 307	2	3 607	5	3 919	3
2 053	2	2 351	13	2 677	2	2 963	2	3 313	10	3 613	2	3 923	2
2 063	5	2 357	2	2 683	2	2 969	3	3 319	6	3 617	3	3 929	3
2 069	2	2 371	2	2 687	5	2 971	10	3 323	2	3 623	5	3 931	2
2 081	3	2 377	5	2 689	19	2 999	17	3 329	3	3 631	21	3 943	3
2 083	2	2 381	3	2 693	2	3 001	14	3 331	3	3 637	2	3 947	2
2 087	5	2 383	5	2 699	2	3 011	2	3 343	5	3 643	2	3 967	6
2 089	7	2 389	2	2 707	2	3 019	2	3 347	2	3 659	2	3 989	2
2 099	2	2 393	3	2 711	7	3 023	5	3 359	11	3 671	13		
2 111	7	2 399	11	2 713	5	3 037	2	3 361	22	3 673	5		
2 113	5	2 411	6	2 719	3	3 041	3	3 371	2	3 677	2		